



Fraunhofer Institut
Naturwissenschaftlich-
Technische Trendanalysen

**Betrachtungen zum Risikobegriff
vor dem Hintergrund
naturwissenschaftlich-technischer Entwicklungen
und staatlicher Planung und Vorsorge**

Uwe Wiemken

August 2004

Die in dieser losen Folge von Publikationen erscheinenden Aufsätze haben das Ziel, einen Beitrag zum Diskurs über langfristige technologische Entwicklungen und ihre Implikationen zu leisten. Sie sollen das fachlich eingegrenzte Angebot des Institutes um allgemeine Aspekte des gesellschaftlichen Wandels ergänzen. Einige dieser Arbeiten, die nicht urheberrechtlich gebunden sind, liegen in gekürzten oder modifizierten Versionen in anderen Publikationen vor.

Der hier neu (2009) herausgegebene Aufsatz ist die lediglich redaktionell modifizierte Neuauflage eines Aufsatzes aus dem Jahr 2004.

Einige Formulierungen, die eine fachwissenschaftliche Facette haben, wären heute „durch besseres Wissen“ zu ersetzen. Darauf wurde verzichtet, um den Zeitbezug zu erhalten. Auch ist klarzustellen, dass der Aufsatz kein Beitrag zum wissenschaftlichen Diskurs ist.

neu herausgegeben 2009

© Uwe Wiemken 2004

Fraunhofer-Institut
für Naturwissenschaftlich-Technische Trendanalysen
Appelsgarten 2
53879 Euskirchen
Telefon +49 2251 18-0
info@int.fraunhofer.de
www.int.fraunhofer.de

Inhalt

1	Hintergrund	1
1.1	Handeln unter Unsicherheit - definitorische Aspekte	3
1.2	Risikomanagement/Risikopolitik	7
2	Die Rolle der technologischen Entwicklungen.....	11
3	Risiko aus Sicht der Planung	15
3.1	Rationale Risiko- und Verwundbarkeitsanalyse.....	15
3.2	Risikomanagement	17
4	Zusammenfassung	20

1 Hintergrund

Der Terroranschlag am 11. September 2001 gegen die USA hat eine bis dahin zwar nicht ungedachte, wohl aber in Ausmaß und Folgewirkung nicht vorhergesehene Bedrohung in das Zentrum der internationalen Politik gebracht und zur Zeit erleben wir „klassische“ Terrorattacken in Form von Bomben- und Brandanschlägen oder durch direkten Missbrauch militärischen Geräts. Darüber hinaus jedoch reicht das Spektrum nicht unrealistischer neu wahrgenommener Gefährdungen von der Einbringung radioaktiver Aerosole in die Klimaanlage von Hochhäusern, die dadurch abrisssreif gemacht werden können, über die Vergiftung von Lebensmitteln oder der lokalen Wasserversorgung durch chemische Agenzien, bis zur Auslösung von verheerenden Epidemien mit vielen Opfern oder der Verursachung des Absturzes von zivilen Verkehrsmaschinen durch Mikrowellen. Auch „nicht-gewalttätige“ Angriffe etwa auf die informationstechnische Infrastruktur eines Landes, d.h. seine Fähigkeit zu kommunizieren und Abläufe zu steuern, können große Schäden hervorrufen. Der 11. September ist darüber hinaus ein erschreckendes Beispiel für den Missbrauch ziviler Technologien.

Viele dieser Bedrohungen hängen mit der Verfügbarkeit neuer technologischer Optionen zusammen oder nehmen vor dem Hintergrund unserer technologisch dominierten Welt neue Formen an. Um vorsorglich und planerisch die Sicherheit der Gemeinschaft zu erhalten, sind seither auch sogar Szenarien in der Planung zu bedenken, die in ihrer katastrophalen Wirkung mit Szenarien des Kalten Krieges vergleichbar sind, und die bisher als nicht ernsthaft vorstellbar ignoriert wurden. Sie wurden letzten Endes als ein „Super-GAU¹“ in der Vorsorge planerisch nicht mehr berücksichtigt.

Alle mit Sicherheitsvorsorge befassten staatlichen Einrichtungen (im gesamten Spektrum der Ressorts) sind derzeit gezwungen, die in ihrem Zuständigkeitsbereich liegenden Maßnahmenkataloge, Planungen und Konzepte einer grundsätzlichen Neubewertung zu unterziehen. Insbesondere müssen die Charakteristika der Bedrohung und des Kriegs-/Konfliktbildes herausgearbeitet werden, von denen alle planerischen Maßnahmen ausgehen.

Die Einschätzung, welche Sicherheitsbedürfnisse gegenüber welchen Bedrohungen die Gesellschaft hat, und durch vorsorgliche Planung befriedigen kann und will, ist gerade heute nicht Ausdruck statischer Einstufung und muss in

¹ GAU = Größter Anzunehmender Unfall, als das schlimmste Ereignis, für das noch Vorsorge getroffen werden kann und muss. Der „Super-GAU“ ist „Schicksal“.

regelmäßigen Abständen erneut geprüft und vor allem explizit formuliert werden. Insbesondere die Frage, welcher Aufwand für die Abwehr welchen Risikos getrieben werden sollte, hängt erfahrungsgemäß stark von der wirtschaftlichen Situation der Mitbürgerinnen und Mitbürger und damit des Staates ab.

Vorsorge bedeutet immer Aufwand, Geld (oder auch Risiko) in einer Zeit, in der man (noch) nicht leidet, und ohne dass man sicher ist, ob man leiden wird (das Geld also „verschwendet“ wäre).

Die Risikowahrnehmung in der Gesellschaft, die letzten Endes den politisch gewollten Aufwand bestimmt, ist in großem Maße vom Zeitgeist abhängig. Welches Risiko letzten Endes als „unvermeidliches zivilisationsbedingtes persönliches Risiko“ einfach hingenommen wird, muss immer wieder neu definiert werden und kann sich wandeln. Der Automobilverkehr weltweit z.B. fordert ein Vielfaches an Opfern in jedem Jahr im Vergleich zu allen terroristischen Angriffen und einer Vielzahl von Risiken, die Schlagzeilen beanspruchen, zusammen. Trotzdem gibt es einen gesellschaftlichen Konsens, dass man zwar vorbeugenden Aufwand treiben und eine beträchtliche Summe dafür ausgeben will, die Risiken zu mindern, dass aber eine gewisse Zahl an Opfern hingenommen werden muss, da man nicht ganz grundsätzliche Paradigmenwechsel in der Gesellschaft einleiten will. Bei der Kernenergie tritt ein vergleichbares Problem auf, wenn die Gesellschaft zu entscheiden hat, welches (in der Kernenergie unvermeidliche) Restrisiko für einen außerordentlich großen Schaden sie gegenüber einem sehr großen ökonomischen und (im „Normalbetrieb“) ökologischen Nutzen bereit ist zu tragen. Wir wissen, dass diese Frage in Abhängigkeit vom Wohlstand der Bevölkerung in unterschiedlichen Ländern ganz unterschiedlich beantwortet wird. Besonders deutlich wird das Vorsorge-Dilemma unter dem Aspekt der Unsicherheit beim Impfproblem, wo man die Vermeidung eines großen Schadens (einer Epidemie) durch einen „kleinen“ Schaden möglicher Impfkomplicationen erkaufen kann (dieses Problem ist in der Mitte des achtzehnten Jahrhundert bei einer damaligen Pockenimpf-Sterberate von einem halben Prozent (!) ausgiebig diskutiert worden²).

Wichtiger Bestandteil des Problembewusstseins ist die Charakterisierung (wenn schon nicht präzise Definition) des Risikobegriffs in seiner objektiven aber auch in seiner subjektiven Ausprägung. Insbesondere die Risikowahrnehmung durch die Bürger bzw. durch die ganze Gesellschaft (über die Medien), durch die sich ein völlig anderer Blickwinkel ergibt, muss in die Betrachtungen einbezogen werden. Die Wahrnehmung entkoppelt den in der wissenschaftlich-technischen Welt weitgehend wohldefinierten Zugang zu diesen Fragestellungen von dem

² Gigerenzer et.al: „Das Reich des Zufalls“, Spektrum Akademischer Verlag, Heidelberg Berlin, 1999

irrationalen Element, das in realen Entscheidungs- und Planungssituationen so häufig dominant ist, und wo es dann in erster Linie darum geht, wie man mit der (auch irrationalen) Risikowahrnehmung der Bürger möglichst rational umgehen kann. Risikoanalyse, Risikowahrnehmung/Risikoakzeptanz und Risikopolitik/Risikomanagement sind ganz unterschiedliche Grundkonzepte und Facetten im Umgang mit unsicherem Wissen in der Planung.

1.1 Handeln unter Unsicherheit - definitorische Aspekte

Wie auch immer man den Begriff Risiko mit seinen Varianten Zukunftswissen, Erwartung, Wahrscheinlichkeit und Zufall definieren wird, alle haben etwas damit zu tun, dass wir, um zu handeln oder langfristig zu planen, implizit oder explizit Voraussagen, mindestens aber Annahmen über die Zukunft - unsere Erwartung - machen müssen. Handeln ist grundsätzlich mit Abstufungen ein „Handeln unter Unsicherheit“.

Gewöhnlich teilt man die „Grade der Gewissheit“ für die „Erwartbarkeit“ eines Ereignisses verschiedenen Klassen zu, die historisch mit der sich in der abendländischen Welt entwickelnden rationalen Weltansicht verknüpft sind:

Physikalische Theorie als Maximum der Objektivierbarkeit und Aussagensicherheit

Wir haben die Erfahrung, dass (validierte) naturwissenschaftliche Theorien und ihre technischen Anwendungen unvergleichliche Vorhersagesicherheit über zu erwartende Ereignisse - z.B. den Ausgang eines Experimentes oder den Bau einer Brücke - bieten (und darum geht es in der Planung). Dies gilt auch für Fälle, in denen ein Spektrum von Ereignissen eintreten kann. Ein Beispiel für letzteres ist der (ideale) Würfel, bei dem aus Symmetriebetrachtungen hervorgeht, dass zwar nicht das Einzelereignis vorhergesagt werden kann, wohl aber die Trefferhäufigkeit bei einer großen Zahl von Versuchen. Dies findet sich in wohldefinierten Wahrscheinlichkeitsverteilungen wieder, mit denen man rational umgehen kann. Wir gehen (in pragmatischer Interpretation) davon aus, dass wir es bei diesem Typ von Vorhersage mit einer letztlich unvermeidlichen Aussagenunsicherheit zu tun haben, die uns die Wirklichkeit vorgibt.

Statistik als Sammlung von Häufigkeiten von Ereignissen aus der Erfahrungswelt

Wir haben im planerischen Handeln zwar häufig keine den Naturwissenschaften vergleichbare Theorie, wohl aber Erfahrung in Form von Statistiken bzw. Informationssammlungen. Statistiken über Sterbefälle waren die frühen empirischen Grundlagen für die Versicherungswirtschaft. Wir wissen mit hoher Sicherheit, dass z.B. Kraftfahrer nur sehr selten während der Fahrt einschlafen

oder einen Infarkt erleiden und wir gehen davon aus, dass die Wahrscheinlichkeit dafür so gering ist, dass wir eine mobile Gesellschaft auf der Basis der Nutzung von Automobilen „riskieren“ können. Natürlich setzen wir dabei die langfristige Stabilität des „statistischen Könnens oder Verhaltens“ der Fahrer voraus, obwohl es sich durchaus ändern kann. Letzten Endes steckt hierin die Annahme, dass wir die inneren Gesetzmäßigkeiten der Mitglieder eines großen Ensembles, die zu ihrem „zufälligen“ Ausfall führen können, nicht sicher kennen, dass aber die Statistik einer genügend große Zahl von „Ereignissen“ diese inneren Gesetze zumindest teilweise widerspiegelt. Mit dieser Interpretation wird der „Ausfall“ einer Person im System wie der Ausfall einer technischen Komponente mit einer angenommenen Ausfallwahrscheinlichkeit behandelt.

Diese beiden Klassen begründen das heute erreichbare Maximum an empirischem „Wissen über die Welt“ und daraus abgeleiteter Planungssicherheit. Sie haben (in Abstufung) in den letzten drei Jahrhunderten zu einer „Durchrationalisierung“ der westlich orientierten Welt geführt und die heutige komplexe Zivilisation ermöglicht. Insbesondere wurde im siebzehnten und achtzehnten Jahrhundert die Begriffsbildung zum „vernünftigen Handeln“ an derartigen Vorstellungen orientiert. Der Merkantilismus/Kameralismus, der ja im Prinzip übergeordnete staatliche Planung möglich machen soll, ist Ausdruck dieser zunehmenden „Vernunft“ im achtzehnten Jahrhundert und der erreichte Bestand an objektivierbarem Wissen über die Welt bildet letztlich die organisatorisch-planerische Basis aller rationalen Entscheidungsprozesse.

Der so umrissene Zugang ist die wichtigste Grundlage jeglicher Risikobetrachtungen, die etwa die Versicherungswirtschaft anstellen muss, bzw. jede Solidargemeinschaft, die sich vor „zufälligen“, nicht fest planbaren Ereignissen schützen, bzw. auf ihre Folgen vorbereitet sein will. Diese Betrachtungsweise spiegelt den rationalen Aspekt wider, auf den wir uns zunächst abstützen können (und müssen!), wollen wir „ein funktionsfähiges (großes) Gemeinwesen“ praktisch organisieren und planen. Daneben gibt es eine umfassende und seit den sechziger Jahren mit der Kernenergieproblemstellung sich immer weiter verallgemeinernde und ausdehnende akademische Diskussion der Gesamtproblematik „risikobehaftetes Handeln unter Unsicherheit“ mit all ihren Facetten, die aber nach meiner Einschätzung noch nicht sehr weit in die Praxis vorgedrungen ist.

Auf der Grundlage der beschriebenen zwei Klassen ergibt sich ein „Ungewissheitsproblem“ aus der Sicht von Vorsorge und Planung, das sowohl grundsätzlicher als auch praktischer Natur ist. Auch in einer im Sinne des „Wissens“ im Prinzip klaren Situation kann die reale Beherrschbarkeit in Frage gestellt sein, weil die relevanten Fragen so großen analytischen Aufwand erfordern, dass sie sich der Praxis entziehen. Diese Problemtypen definieren sich deshalb letzten Endes aus dem, was mit technologischem Fortschritt (nicht unbedingt Erkennt-

nisgewinn) die Beherrschung immer komplexerer Situationen stützt. Es gibt viele Fälle, in denen realistisches Wissen aus den obigen Klassen unstrittig vorhanden (oder beschaffbar) ist und auch methodisch klar ist, wie man „im Prinzip“ zu einer aggregierten Aussage kommen kann. Ein Beispiel hierfür ist die Wettervorhersage, der zwar letzten Endes ein vollständig physikalisches Modell zugrunde liegt, bei der aber eine sehr große Menge an Daten und Zusammenhängen zu berücksichtigen sind. Diese extreme Komplexität setzt der tatsächlichen modellhaften Berechenbarkeit und Prognosemöglichkeit Grenzen durch die sog. „Kombinatorikexplosion“. Ebenso können Nichtlinearitäten in den Zusammenhängen zu Systemzuständen führen, die sich - auch bei deterministisch angenommener Basis - als völlig unvorhersagbar, als „chaotisch“ erweisen. Rein kombinatorische Probleme treten bei der Analyse qualitativer Daten auf. Hier hat man es häufig mit einer Skalenqualität (etwa nur mit Nominal- oder Ordinalskalen) zu tun, die sich einer analytischen Behandlung entziehen. Hier soll keine grundsätzliche Diskussion vorgenommen werden, es muss aber festgehalten werden, dass eine (technologiegetriebene³) Situation entstanden ist, bei der die grundsätzlichen Beschränkungen in der Modellierung einerseits zwar vorhanden sind, durch die Möglichkeiten der „Computational Science“ in der Praxis aber immer weiter hinausgeschoben werden. Es ist heute möglich, immer komplexere Fragestellungen modellhaft zu beschreiben und damit „fortzuschreiben“ - d.h. zu prognostizieren (s. u.).

Deutlich abzusetzen (wenn auch mit fließendem Übergang) ist schließlich eine Klasse von „Vorhersageproblemen“ (in gewissem Sinne der „verbleibende Rest“), mit denen Institutionen konfrontiert sind, die für staatliche (aber auch unternehmerische) Vorsorge und Planung verantwortlich sind:

Zufall und subjektive Wahrscheinlichkeit

Hier wird die Situation „unübersichtlich“. Wenn es um Schadensereignisse geht, die „genau so noch nie oder nur vereinzelt“ tatsächlich eingetreten sind, haben wir ja grundsätzlich keine „statistischen“ Daten, und nur in den wenigsten Fällen steht uns das „Vorhersageinstrument der o.g. physikalisch basierten Weltbilder“ zur Verfügung. Wir müssen sie letztlich in Ermangelung besserer Kenntnis als Zufall ansehen. Wenn man so will, ist dies die Domäne des „der Mensch denkt, und Gott lenkt“ oder der „höheren Gewalt“, sofern man den Zufall einem „höheren“ Eingriff zuschreibt. In nüchternerer Betrachtung könnte man als „quasi-statistische“ Referenz „ähnliche“ Ereignisse heranziehen, die schon einmal passiert sind und sich an deren statistischer Häufigkeit orientieren (was immer „ähnlich“ bedeutet). Letzten Endes setzen wir voraus, dass die all-

³ Moore's Law und ein erwarteter Leistungsanstieg um den Faktor 1000 in den nächsten zehn bis fünfzehn Jahren

gemeine Erfahrung, die wir als Individuen und als Gesellschaft über „lange“ Zeiträume ansammeln, etwas über „die Wahrscheinlichkeit oder die Erwartbarkeit“ des Eintretens von Schadensereignissen in der Zukunft widerspiegelt. Hier kommt der Begriff der subjektiven Wahrscheinlichkeit ins Spiel. Um den formalen Umgang etwa in Entscheidungs- oder Bewertungsmodellen zu erhalten wurde/wird ein solcher Wahrscheinlichkeitswert häufig wie eine naturwissenschaftlich oder statistisch begründete Wahrscheinlichkeit in Planungen einbezogen. Dies ist ein erkenntniskritisch sehr bedenklicher Prozess, da man sich bewusst bleiben sollte, dass eine grundsätzliche Unsicherheit und damit ein persönliches Risiko bei planerischen Entscheidungen auf der Basis von „Meinung“ (statt Wissen) unvermeidlich ist. Vor allem kann man sich als Entscheidungsträger hier nicht auf einen vermeintlich „objektiven“ Tatbestand berufen, der die Entscheidung „erzwungen“ hat, sondern muss die Verantwortung persönlich tragen. In der Regel wird dies auf der Grundlage der intuitiven subjektiven Einschätzung (und Risikobereitschaft) beruhen. Diese Betrachtungsweise ist natürlich uralte und war Grundlage jeder „vorsorglichen Planung“, lange bevor wissenschaftliche/mathematische Wahrscheinlichkeitsbetrachtungen im siebzehnten Jahrhundert einsetzten.

Einen ganz anderen Charakter bekommen rationale Risikobetrachtungen, wenn wir uns fragen, wie denn der Staat oder ein Unternehmen konkret planerisch mit dem Risiko umgeht, dass etwas nicht Vorhergesehenes, Zufälliges geschehen kann, und wie man sich auf diesen Fall vorbereitet. Für dieses Risikomanagement kann man mehrere Grundzüge unterscheiden (s.u.). Letztlich soll analysiert werden, was man rational tun kann, auch wenn ein empirisch abgesicherter Risikozugang im obigen Sinne nicht erreichen werden kann (allenfalls in dem Sinne, dass man sich im Rahmen des „Denkbaren“ und des „gesunden Menschenverstandes“ bewegt).

Alle Formen des Umganges mit Risiko werden überlagert von der Tatsache, dass die Wahrnehmung der Menschen da, wo sie direkt betroffen sind, häufig fast überhaupt nichts mit objektiven Gegebenheiten zu tun hat. Vor allem ist das Maß, mit dem man eine „größer - kleiner - Skala“ definieren könnte, im Alltag für intuitive Situationen fast nicht vorhanden, und schon gar nicht mit den rationalen Ansätzen wie „Risiko = Eintreffwahrscheinlichkeit x Schadenshöhe“ zu beschreiben. Kleine Schäden, die sicher sind, werden fast immer als negativer eingestuft als große Schäden, die vielleicht in der Zukunft auftreten können, und häufig steht die Schadenswahrnehmung in keinem sinnvollen Zusammenhang mit den realen Gegebenheiten. Auch im politischen Alltag spielt die reale Wahrscheinlichkeit eines Schadens und seine rationale Bewertung sehr häufig lediglich eine untergeordnete Rolle - entweder, weil der Politiker selber eine nichtrationale Wahrnehmung hat, oder weil die irrationalen Ein-

schätzungen seiner Wähler für ihn eine (nun wiederum rationale) Randbedingung darstellt.

Insbesondere unsere (heutige) Risikowahrnehmung (in Deutschland) setzt eine Risikobeherrschung wie im rationalen Bereich voraus. Wir glauben, dass der Staat alles im Griff haben muss und letztlich alle Probleme auch lösbar sind (und evtl. nehmen die Politiker das genauso wahr). Diese Erwartungshaltung ist sicher falsch. Andere Staaten wie z.B. die USA haben eine viel ursprünglichere Wahrnehmung des Lebens und seiner Gefahren. Auch der Glaube, dass der zivilisatorische Prozess (der „Fortschritt“ des neunzehnten Jahrhunderts) eine monoton steigende Funktion sein muss, ist nicht belegbar.

1.2 Risikomanagement/Risikopolitik

Im Prinzip können Schadensbetrachtungen völlig unabhängig vorgenommen werden von unserem „mehr oder weniger“ Wissen, ob und aus welchen Ursachen heraus Schadensereignisse tatsächlich eintreten. Das Unternehmen (oder der Staat) führt eine Analyse durch, welches Spektrum von Schadensereignissen als möglich eingestuft wird - eine Verwundbarkeitsanalyse - und bereitet sich durch Planung darauf vor, ohne zu fragen, welches Ereignis mit welcher Wahrscheinlichkeit auftritt. Ziel wäre dann, grundsätzlich das Unternehmen weniger verwundbar zu machen. Hierfür bieten sich verschiedene Strategien an.

Die naheliegendste Möglichkeit zur Schadensvermeidung bzw. -minimierung besteht natürlich in individuellen Verhaltensänderungen. Diese „taktisch/operationelle“ Reaktion hat z.B. in den sechziger Jahren des vorigen Jahrhunderts zu einer großflächigeren Dislozierung von Streitkräften geführt, nachdem mit Nuklearwaffen auf dem Gefechtsfeld gerechnet werden musste. In den siebziger Jahren wurden analoge Untersuchungen darüber durchgeführt, mit welchen Implikationen für das taktische Verhalten der Truppe durch neue Technologien wie die sog. PGM⁴ zu rechnen sein würde. Auch in unseren Tagen wird das Verhalten von Soldaten immer wieder der veränderten Bedrohung angepasst. Ebenfalls hierher gehört es, wenn etwa wichtige Amtsträger nicht in kritischer Anzahl und womöglich einschließlich Stellvertretung in einem Flugzeug reisen, oder wenn man darüber nachdenkt, ob die gewaltigen Konzentrationen von Menschen in Hochhäusern nicht ein allzu großes Schadenspotential darstellen. Allerdings gibt es für solche Vermeidungsstrategien offensichtliche Grenzen, wenn Verhaltensänderungen die notwendige Funktionsfähigkeit des „Gesamtsystems“ auf der „Verteidigerseite“ zu stark beeinträchtigt oder gar zu ungewollten „Umklappprozessen“ führen. In der Tat ist es eine der großen Sorgen der westlichen Welt, dass der Tourismus durch den Terrorismus so

⁴ PGM = Precision Guided Munition

abgeschreckt werden könnte, dass die komplexen weltwirtschaftlichen Zusammenhänge nachhaltig gestört werden - gerade am stärksten zum Nachteil der unterentwickelten Länder.

Eine rationale Vorgehensweise im Rahmen von Risikomanagement kann auch darin bestehen, dass unabhängig von der Form und Wahrscheinlichkeit der Bedrohung für alle insbesondere technischen Prozesse und Abläufe „Inhärente Sicherheit“ zu einem Designkriterium gemacht wird, d.h., dass der Schaden unabhängig von der Eintrittswahrscheinlichkeit vergleichsweise klein gehalten wird oder gar nicht auftreten kann. Ein Beispiel sind etwa neue Kernreaktor-konzepte, bei denen z.B. grundsätzlich keine Kernschmelze möglich ist. Solche „Unfallverhütungsstrategien“ sind natürlich wohlvertrauter Bestandteil von Unfallverhütungsvorschriften, durch die Unfälle auch unter Einbeziehung von denkbarem menschlichem Versagen so unwahrscheinlich wie möglich gemacht werden sollen. Bei modernen Papierschlagscheren muss man sich Mühe geben, wenn man sich verletzen will, wir streben an, alle Tanker mit einer Doppelwandung zu versehen oder wir beschaffen Munition, die auch bei Beschuss nicht zur Zündung gebracht werden kann (LOVA). Hierzu gehören auch die Überlegungen, Flugzeugcockpits vom Passagierraum aus unzugänglich zu machen, oder von der Bodenstation eine Fernsteuerung des Flugzeuges erzwingen zu können mit dem Ziel, größeren Schaden zu verhindern. Es soll unabhängig von äußeren Einwirkungen oder der Risikobereitschaft des Bedieners bzw. des Entscheidungsträgers erreicht werden, dass technische Anlagen „als Selbstzweck“ keine oder verringerte Risikopotentiale enthalten. Sie sollen nach Möglichkeit „idiotensicher“ sein und keine gefährlichen Betriebszustände zulassen. Eine Variante dieser Strategie besteht in der Schadensminimierung (wenn man ihn nicht verhindern kann). Man wird Schotten in Schiffe einbauen, die Arbeitsstätten in Munitionsfabriken so anordnen, dass bei einer Explosion immer nur kleine Einheiten betroffen sein können, und man könnte allzu große Konzentration von Menschen in Hochhäusern vermeiden. Hier wird aber schon deutlich, dass manche Risiken nur durch einen grundsätzlichen Wandel zuverlässig vermieden werden können, und dass man sich leisten können muss, eine so hohe technische Sicherheitskultur zu formulieren und zu realisieren. Wenn sich darüber hinaus die Risiken letztlich auf absichtsvolles aggressives Verhalten zurückführen lassen, kommt die Frage ins Spiel, wie weit man sich erpressen lassen kann.

In den Fällen, wo die Unsicherheit aus den nicht bekannten Absichten eines Gegners resultiert, haben rationale Strategien in der Vergangenheit zu dem bekannten Rüstungswettlauf geführt, der erst wieder auf einer sehr übergeordneten Ebene der Betrachtung als unsinnig entlarvt werden kann. Grundsätzlich aber ist auch das eine mögliche Ausrichtung, die eine rationale Basis hat. Wenn man grundsätzlich weitaus stärker ist als jeder mögliche Gegner, wird

man (innerhalb der angenommenen Auseinandersetzungsformen) sicherer sein, als wenn man schwächer ist, unabhängig von seinen tatsächlichen Absichten. Man kann dies als eine Strategie zur „Verstärkung der Asymmetrie“ bezeichnen. Der Betrieb und die Sicherung der weltweiten IT-Netze ist derzeit ein Feld für solche übergeordneten Strategien. Um sicher zu gehen, dass es niemanden gibt, der bei Organisation, Betrieb und Überwachung (und natürlich Nutzung aus Eigeninteresse) solcher Netze überlegen ist, investieren die USA auf den relevanten Gebieten sehr hohe staatliche Summen in Forschung und Entwicklung. Es werden darüber hinaus im täglichen Betrieb (kleinere) Risiken bewusst in Kauf genommen, um in der Auseinandersetzung mit Angreifern möglichst umfangreiche Erfahrung zu gewinnen.

Es ist möglich, den Abwehraufwand so hoch zu treiben, dass mögliche Gegner mit immer größeren Ansprüchen an Vorbereitung und Planung und damit an Intellekt und rationalem Verhalten konfrontiert werden, um noch erfolgreich wirklich große Schäden zu verursachen. Beispiele sind die ununterbrochenen Kontrollen von Gleisanlagen oder die Einführung von Flugbegleitern. Dies könnte gerade im Terrorismusbereich dazu führen, dass die Bedrohung sich auf die „Nadelstiche“ individueller und damit begrenzter Einzelhandlungen reduzieren lässt. Relativierend muss man natürlich sagen, dass der 11.9.2001 klar gemacht hat, dass ein fundamentalistisches „Weltbild“ bis hin zur Bereitschaft zum Selbstmord offenbar auch in einer Ausbildung im einem empirisch-rationalen Umfeld aufrecht erhalten werden kann. Trotzdem dürfte dieser Personenkreis in der „Szene“ nicht sehr häufig sein. Auch diese Aufwandvariante ist natürlich nicht billig, da die gesamte „Grenze“ (im übertragenen Sinne) geschützt werden muss und der Gegner alle Angreifervorteile hat.

Schließlich besteht eine weitere (wenn auch eine nahezu triviale) grundsätzliche strategische Ausrichtung bei Unsicherheit darin, das Maß der Unkenntnis bei den Einflussfaktoren zu reduzieren, d.h., die identifizierbaren rationalen Einflussgrößen in ihrer Bedeutung für das Auftreten von Schäden zu stärken (also keine Traumdeuter und Astrologen zu Rate zu ziehen). Diese etwas abstrakte Formulierung sei ergänzt durch den Hinweis, dass hier natürlich insbesondere die „harte Faktenbasis“ im Sinne von „operativen Datenbanken“ der Kriminalämter oder der Dienste gemeint ist. Diese Analysebasis bedingt Forschung, operative Aufklärung und Fähigkeit zur ad-hoc Situationsanalyse. Sie bedarf natürlich der gesellschaftlichen Meinungsbildung, ob man solche „Wissensansammlungen“ in der Hand des Staates zulassen will oder lieber ein Alltagsrisiko z.B. vergleichbar mit dem Verkehrsrisiko (mit einigen tausend Toten im Jahr) in Kauf nehmen will (diese Alternative ist ernst gemeint).

In der Regel werden die genannten Strategien da, wo sie keine rational abgeleitete Grundlage haben, auf der intuitiven subjektiven Einschätzung/Priorisierung (und Risikobereitschaft) von Politikern oder des Unternehmers beruhen („soll

der Staat Geld investieren, um ein Warn- und Verteidigungssystem gegen die Meteoritenbedrohung aufzubauen?"; „soll der Staat Streitkräfte bereithalten, um sich gegen eine mögliche Bedrohung schützen zu können?"). Diese Betrachtungsweise ist natürlich uralte und war implizit Grundlage jeder „vorsorglichen Planung“, lange bevor wissenschaftliche/mathematische Wahrscheinlichkeitsbetrachtungen im siebzehnten Jahrhundert einsetzten. Im Grunde sind ja auch Katastrophenschutz oder Streitkräfte vorsorgliche Institutionen, die „für alle Fälle“ je nach persönlicher Situationseinschätzung durch die Entscheidungsträger als Ordnungskräfte eingerichtet werden (der Fall, dass man bereits vor hat, Krieg zu führen, sei hier nicht angenommen). Begrifflich deutlich ist dieser individualisierte Umgang mit dem Risiko bei den sog. aleatorischen Verträgen⁵, bei denen von den Vertragspartnern eine ganz persönliche „Wette mit dem Schicksal“ (oder dem Zufall) abgeschlossen wurde, z.B. bei der Ausrüstung von hochriskanten Handelsexpeditionen im sechzehnten Jahrhundert, bei denen ein sehr hoher Gewinn einem Totalverlust gegenüber stand.

Entscheidend ist die Tatsache, dass dem Entscheidungsträger (und auch einer kritischen Öffentlichkeit) klar sein muss, dass es Fälle geben kann, wo es keine Referenz einer rationalen Risikoanalyse gibt, und Entscheidungen unvermeidlich auf einer subjektiven Risikowahrnehmung beruhen. Der Verantwortung können sich Entscheidungsträger in der „wahren Welt“ in nur wenigen Fällen dadurch entziehen, dass sie sich auf „eine objektive Sachlage und unausweichliche Sachzwänge“ berufen - auch wenn sie das gerne tun.

⁵ d.h. „vom Zufall abhängigen“

2 Die Rolle der technologischen Entwicklungen

Die technologischen Entwicklungen haben in den letzten 250 Jahren (seit Beginn der „Industriellen Revolution“ in England) immer mehr und mit zunehmender Dynamik Einfluss auf die wirtschaftliche und kulturelle Entwicklung der Gesellschaft in den industrialisierten Ländern genommen. Auf der einen Seite erleben wir dabei einen bis dahin für die überwiegende Mehrheit der Bevölkerung unvorstellbaren Wohlstand mit einem hohen Maß an Freiheit, Selbstbestimmung und Sicherheit. Auf der anderen Seite treten neue Bedrohungen auf; kurzfristig und unmittelbar durch neue „Macht, Schaden anzurichten“ in Händen, die diese früher nicht hatten, und langfristig und indirekt durch den erzeugten gesamtgesellschaftlichen Veränderungsdruck, der den Menschen schwierige Anpassungen in kurzer Zeit - und damit schnelles Handeln - abverlangt. Die Geschichte zeigt, dass gerade solche Anpassungsprozesse Ursache für gewaltsame Konflikte sowohl innerhalb einer Gesellschaft, als auch in ihrem Außenverhältnis waren. Vor diesem Hintergrund ist die belastbare Beobachtung, Analyse und Prognose der zugrunde liegenden naturwissenschaftlichen und technologischen Entwicklungen eine zentrale Notwendigkeit, wenn man mit staatlichem Handeln nicht lediglich auf vollzogene und erst dann in ihren Auswirkungen erkennbare Entwicklungen reagieren will.

Wenn auch alle technologischen Entwicklungen von Menschen gewollt, entschieden und durchgeführt werden, ist es wohl eine historische Erfahrung, dass sie in ihrer Summe mit einer personenunabhängigen, „anonymen“ Dynamik ablaufen. Der bewusste Verzicht auf eine Technologie, die gleichzeitig Vorteile und Nachteile verspricht, ist nur äußerst selten „aus Einsicht“ vorgenommen worden und hat so gut wie nie lange angedauert. Es ist deshalb nicht prinzipiell, aber aus planerischer/vorsorglicher Sicht sinnvoll, anzunehmen, dass alles, was technologisch möglich ist (und ein „Nutzenversprechen“ in sich birgt), auch berücksichtigt werden muss. Man darf sich nicht völlig darauf verlassen, dass Bedrohungen „aus Vernunft“ unter Kontrolle gehalten werden. Aus Sicht einer vorsorglichen Planung laufen nützliche (für wen auch immer) technologische Entwicklungen mit hoher anonymer Eigendynamik ab. Es ist nicht damit zu rechnen, dass die negativen Implikationen, die man vorhersagen mag, sie verhindern. Versuche, sie zu steuern und zu kontrollieren sind natürlich unbenommen, aber nur sehr begrenzt wirksam.

Die Zivilisation unserer Tage weist in der Folge der technologischen Entwicklung sowohl im historischen als auch im globalen Vergleich ein Höchstmaß an Sicherheit für Leib und Leben ihrer Bürger auf. Das hat dazu geführt, dass die Lebenserwartung in den letzten zwei Jahrhunderten kontinuierlich gestiegen ist (sinkendes Individualrisiko) und eine Situation entstand, in der dies als selbstver-

ständig und als natürliches Recht empfunden wird. Alle Bedrohungen dieser Sicherheit werden als besonders gravierend empfunden und der Schutz des individuellen Menschenlebens gilt (meistens noch vor der Freiheit und Menschenwürde) als das höchste Gut, das der Staat schützen muss (nahezu „koste es, was es wolle“).

Gleichzeitig haben sich in den Industrienationen besonders in vielen zivilen Einrichtungen und Abläufen große Gefahrenpotentiale angesammelt, die durch technische Sicherheitseinrichtungen, letzten Endes aber durch „Kenntnis, Einsicht und Selbstschutzinteresse“, ergänzt durch Vorschriften und entsprechende Schulungen, unter Kontrolle gehalten werden. Dazu zählen z.B. Anlagen der chemischen und nuklearen Industrie oder Labors, die Forschung mit B-Agenzien betreiben, aber auch moderne Verkehrs- oder Transportmittel (wie Tanklastwagen). Auch moderne Waffentechnik bis hin zu ihrem Extrem der Kernwaffen kann man als „Technologie mit hohem Schadenspotential“ auffassen. Schleichend hat sich in den letzten Jahrzehnten darüber hinaus eine problematische Abhängigkeit von IT-basierter Infrastruktur aufgebaut, die ebenfalls bei Ausfall zu einer Gefährdung der Volkswirtschaften führen kann.

Das Gefahrenpotential kann durch „technisches oder menschliches Versagen“ oder durch gezielten Missbrauch⁶ freigesetzt werden. Eine Analyse, welche Technologien im Sinne einer „Waffe“ eingesetzt werden können, und wo überall Bedrohungen aus technologischer Sicht vorhanden sind oder entstehen, kann hier nicht systematisch durchgeführt werden.

Unvermeidlich (jedenfalls ohne Änderung sehr grundlegender Strukturen) in einer modernen Zivilisation ist die Zunahme des möglichen Ausmaßes einer Katastrophe durch die größere „Dichte“ von Menschen (in Hochhäusern, Stadtzentren oder bei Großveranstaltungen - im Großen in Metropolen) oder durch die Ausbreitung eines Schadensmechanismus über die umfassende Verkehrs- und Kommunikationsinfrastruktur.

Wenn Risiken für technische Anlagen und Abläufe als Zufallsereignisse behandelt werden können, kann man im Grundsatz einerseits davon ausgehen, dass auch Konzentrationsprozesse zwar das Zivilisationsrisiko - im Sinne eines Ansteigens der Wahrscheinlichkeit für das Auftretens eines ungewöhnlich großen Schadens bei einem einzelnen Ereignis - steigern können, andererseits aber das Individualrisiko durchaus gleichzeitig gemindert werden kann⁷. Wenn z.B. ein Großraumflugzeug geplant wird, werden große Anstrengungen unter-

⁶ ohne hier die Frage diskutieren zu wollen, wann bei Waffen ein „Missbrauch“ vorliegt.

⁷ Nicht betrachtet wird hier, dass ein großer Schaden durch „diffuses“ gesamtgesellschaftliches Verhalten entstehen kann (Klimawandel, Allergien).

nommen, die Wahrscheinlichkeit technischen oder menschlichen Versagens gegenüber den herkömmlichen Flugzeugen zu senken. Damit wird aber ein einzelner Flug sicherer, obwohl das Schadensereignis (und besonders in der Schadenswahrnehmung) größer wird. So lange man auf der Grundlage der beiden oben beschriebenen höchsten Klassen der Aussagensicherheit fußt, steht einer Fortführung einer „klassischen Risikopolitik“ im Grunde nichts entgegen, wenn der Aufwand auch in diesem „einfachen“ Fall bei immer komplexer werdenden Systemen sehr groß werden kann.

Bis heute haben sich die mit dem zivilisatorischen Fortschritt verknüpften technischen Entwicklungen wie etwa der Straßenverkehr oder die Energieversorgungstechniken noch nicht trendbrechend negativ auf das Individualrisiko, ausgedrückt etwa als Lebenserwartung, ausgewirkt. Jedenfalls haben die risikomindernden Faktoren unserer Zivilisation derzeit noch die Überhand gegenüber den zivilisationsbedingten risikosteigernden Faktoren⁸ - unabhängig davon, wie wir diese Risiken wahrnehmen. Manchen Menschen scheint der Elektrosmog als größere Bedrohung als der Straßenverkehr oder die Sonnenbank. Allerdings kann man wohl auch nicht davon ausgehen, dass sich diese in der Summe positive Entwicklung zwangsläufig in alle Zukunft fortsetzen muss. Es ist durchaus denkbar, dass irgendwann das Risiko, in der Folge eines zivilisationsbedingten Ereignisses zu sterben, zu einer Umkehrung in der Entwicklung der individuellen Lebenserwartung führt. Dies könnte z.B. eintreten, wenn ein in terroristischer Absicht freigesetzter Erreger - ein Zivilisationsrisiko - einen merklichen Teil der Bevölkerung töten würde, und solche Szenarien mit signifikanter Wahrscheinlichkeit „real zu Buche schlagen würden“, d.h. nicht mehr nur vorsorgesteuernde Annahmen wären. Das ultimative Zivilisationsrisiko muss angenommen werden, wenn der Schaden so groß wird, dass die Zivilisation eines Landes oder sogar global nicht weiter aufrecht zu halten wäre. Dann wäre „Zivilisationsrisiko“ als „Risiko für die Zivilisation“ zu interpretieren.

Die andere, im Grundsatz positive Seite technologischer Entwicklungen ist die Tatsache, dass sie Chancen für eine effektivere Bekämpfung der Bedrohungen eröffnen, sowohl bezogen auf nicht gewollte Schäden als auch bezogen auf gewollte Schäden/Angriffe (terroristisch, kriegerisch). Grundsätzlich ist (zumindest nach meiner Einschätzung) eine zivilisatorisch (und technisch) hochentwickelte Gesellschaft eher in der Lage, mit letztlich doch kleinen Gruppierungen von Angreifern fertig zu werden.

Auch ohne eine gründliche Analyse vorwegzunehmen, kann man sagen, dass z.B. die Bereitstellung von „Analysekapazität“ sowie automatisierte oder teilautomatisierte Steuerungs- und Kontrollfunktionen durch moderne und zu erwar-

⁸ Wie etwa die Allergierkrankungen

tende IT-Technologie zu den wichtigsten „unterstützenden“ Technologieentwicklungen gehört. Ein Beispiel ist der Bedarf, kombinatorische Problemstellungen in eine Analyse einbeziehen zu können. Er ist schon heute (im Gegensatz zurzeit vor 30 Jahren) teilweise zu befriedigen. Diese „brute force“-Komponente von „Computational Science“ hat z.B. den Computer zu einem ernsthaften Konkurrenten für Schachgroßmeister gemacht.

Der Wunsch, durch Aufwand und Kreativität, wie sie nur von einer leistungsfähigen Industrienation aufgebracht werden können, einen dauerhaften (und für die Sicherheit ausreichenden) Vorsprung im Schutz gegen „kriminelle Amateure“ zu sichern, ist z.B. integraler Bestandteil der amerikanischen Sicherheits- und Technologiepolitik. Auf diese Weise soll die „unbedingte Dominanz“ des Staates mit seinem Gewaltmonopol im Sinne eines „polizeilichen“ Selbstverständnisses sichergestellt werden. Diese US-nationale Position spiegelt vielleicht eine andere Grundeinstellung im Vergleich zu Deutschland und auch Europa wider, macht aber klar, dass die technologischen Entwicklungen mit ihrem Potential Bestandteil nationaler und europäischer Sicherheitsanalysen und -entwicklungen sein müssen.

Dies schließt übrigens ggf. eigene Waffenforschung mit dem Ziel der Beherrschung des Schutzes auch auf geächteten Gebieten ein, da man andernfalls Gefahr läuft, dass sich böswillige (und skrupellose) Kräfte in einer offenen globalen Gesellschaft Wirkmöglichkeiten verschaffen, denen die Gesellschaft nichts entgegenzusetzen hat. Es muss z.B. eine gründliche Diskussion in der Gesellschaft geben, ob die sich derzeit extrem dynamisch entwickelnde Bio- und Gentechnikforschung mit dem Anwendungspotential in der Biowaffenforschung als unethisch abzulehnen ist, wenn das dazu führen kann, dass sich skrupellose Staaten mindestens ein Erpressungspotential dadurch verschaffen, dass sie offene Information für ein spezialisiertes Waffenprogramm nutzen. Es wäre dann ggf. nicht auszuschließen, dass die Opfer einer Erpressung oder eines Angriffes gar nicht in der Lage wären, eine Bedrohung zu beurteilen oder etwa Gegenmittel zu entwickeln. Eine demokratische Gesellschaft, die sich ja durchaus für eine unbedingte Ächtung und einen völligen Rückzug aus diesem Forschungsbereich entscheiden kann, darf sich aber nicht um die klare Formulierung der Risiken herumdrücken, die damit verbunden sind. Vor allem darf sie eine Entscheidung nicht „in der klammheimlichen Gewissheit“ treffen, dass andere verbündete Staaten „sich schon um das Problem kümmern werden“.

Die Hoffnung, solche technologisch basierten „Wettlaufsituationen“ in Zukunft vermeiden zu können, wird sich sicher nicht vollständig erfüllen. Mindestens muss deshalb eine gründliche Urteilsfähigkeit sicherstellen, dass die Industrienationen nicht von Bedrohungen überrascht werden können, die sich aus zivilen Entwicklungen so „auskoppeln“ lassen, dass Feinde einen signifikanten Vorsprung im „Anwendungsbezug“ erreichen können.

3 Risiko aus Sicht der Planung

Der Grundauftrag aller vorsorglichen Planung besteht darin, auf der Basis dessen, was „man rational weiß“, aber auch dessen, was der Entscheidungsträger „glaubt“, Aufwand zu treiben, um politisch gegebene Ziele zu erreichen. Dabei muss insbesondere staatliche Planung notwendig im Kern rational und realitätsorientiert bleiben, wenn sie auch natürlich die verbreitete Irrationalität oder Inkonsistenz der Welt als Randbedingung einbeziehen muss. Planung in einem modernen Staat bedeutet immer konkretes Handeln in einem extrem komplexen und heterogenen Umfeld. Eine Zunahme der Irrationalität, Sprunghaftigkeit und Willkür wäre eine bedenkliche Gefährdung der Funktionsfähigkeit der Gemeinschaft.

Die Mindestforderung ist deshalb, dass alle beteiligten Vorsorgeinstitutionen aus ihrer Sicht Risiko- und Verwundbarkeitsanalysen vornehmen, mit denen eine rationale Basis für staatliches Risikomanagement bzw. staatliche Risikopolitik gewonnen werden kann.

3.1 Rationale Risiko- und Verwundbarkeitsanalyse

Seit über hundert Jahren ist die rationale Analyse technischer Risiken (d.h. Unfallrisiken) für Anlagen und Systeme wohletablierter Bestandteil von staatlichen Genehmigungsverfahren und vorausschauender Planung. Insbesondere im Zusammenhang mit der Kernenergie wurden begleitend umfangreiche Forschungen durchgeführt, um ein Höchstmaß an Sicherheit in der friedlichen Nutzung der Kernenergie zu erreichen. Es war klar, dass der potentielle Schaden, der hier auch ungewollt auftreten kann, großen Aufwand rechtfertigte und notwendig machte⁹. Dem Risikofaktor „menschliches Versagen“ wurde in der Technik dadurch Rechnung getragen, dass Steuersysteme entwickelt wurden, deren Sicherheit so wenig wie möglich von Menschen abhängig ist, oder Konfigurationen gewählt wurden, die „inhärent sicher“ sind. Diese Grundproblematik ist, wie schon gesagt, vertraut, und beinhaltet Wahrscheinlichkeitsannahmen (im Prinzip) objektiver¹⁰ Art, denen die „Vermutung“ unterlegt wird,

⁹ die sich wandelnde Einschätzung des Sicherheitsproblems in der Kernenergie - etwa in der Erkenntnis der Unvermeidbarkeit eines Restrisikos - führte in der Folge zu einer Vielzahl von „Nachbesserungen der Vorschriften“ und schließlich zum Ausstiegsbeschluss.

¹⁰ Die angenommene Wahrscheinlichkeit, dass es extrem unwahrscheinlich ist, dass die Mitarbeiter eines Biolabors gemeinsam verrückt werden und Schaden anrichten, ist natürlich eine subjektive Wahrscheinlichkeit. Derartige Überlegungen waren aber übrigens durchaus real, als man über

dass diese Werte angenommen würden, wenn viele solche Ereignisse „gemessen und zur Grundlage einer Statistik unabhängiger Ereignisse“ gemacht werden könnten. Schon die Tatsache, dass es Ereignisketten gibt, bei denen voneinander abhängige Wahrscheinlichkeiten behandelt werden müssen, stellt allerdings bei immer komplexeren technischen Systemen eine problematische Einschränkung der Plan- und Beherrschbarkeit dar. Zwar ist das mathematische Instrumentarium durchaus ausreichend, kaum zu lösen ist hingegen aus Gründen der riesigen Zahl von Varianten (Kombinatorikexplosion, s.o.) das Auffinden und Durchdenken aller potentiell gefährlichen Ereignisketten.

Alle so formulierten Zusammenhänge sind jedoch nur sehr begrenzt gültig oder auch nur relevant, wenn man absichtsvolles Verhalten zur Herbeiführung eines möglichst großen Schadens annehmen muss. Dann muss man damit rechnen, dass gerade große Schadenspotentiale besonders „attraktive“ Ziele sind. In einer solchen Situation ist es sicher nicht sinnvoll möglich, Wahrscheinlichkeiten für das Auftreten von Schäden anzugeben, es sei denn als klar subjektive Einschätzungen etwa von Politikern, die dann als Wahrscheinlichkeiten (bzw. als Priorisierung) interpretiert werden könnten. Das aber ist letztlich keine geeignete Planungsgrundlage, da es unvermeidlich Gegenstand der politischen (kurzlebigen) medialen Tagesauseinandersetzungen sein würde, die viel zu viele irrationale Elemente enthalten, um darauf eine stabile Planung aufzubauen.

Wahrscheinlich wird man das Problem der vollständigen Analyse möglicher Ereignisketten in allen technischen Anlagen einschließlich der Angabe von Wahrscheinlichkeiten im Sinne einer „klassischen Risikoanalyse“ aus Aufwandsgründen auf absehbare Zeit nicht lösen können.

Für die rationale Planung ist es deshalb notwendig, als unstrittige Basis die reinen Schadenspotentiale zu identifizieren und so weit möglich nach Höhe (unabhängig von der Auftretenswahrscheinlichkeit) zu charakterisieren. Allerdings steht man auch bei einer solchen Verwundbarkeitsanalyse wieder vor dem Problem der Kombinatorikexplosion. Dieses wird dadurch verschärft, dass man mit bewussten Eingriffen an der „effektivsten“ Stelle einer gedachten Ereigniskette rechnen muss (es ist bezeichnend, dass bei einem Ausfall der Stromversorgung in Italien zunächst nicht ausgeschlossen werden konnte, dass der Beginn der Ereigniskette einen „wohininformierten“ terroristischen Ursprung hatte).

Vor diesem Hintergrund ist eine möglichst vollständige Verwundbarkeitsanalyse anzustreben, die eine wichtige Grundlage für ein vorsorgliches Risikomanage-

Sicherungssysteme nachdachte, mit denen ein Nuklearschlag durch einen geisteskranken Präsidenten verhindert werden sollte.

ment bilden kann. Dazu ist es notwendig, die Schadenspotentiale aller technischen Anlagen, Einrichtungen und Abläufe zu identifizieren, zu analysieren und aus Sicht eines möglichen Schadensumfanges zu bewerten. Ein zweiter Schritt muss darin bestehen, mögliche Mechanismen und Abläufe einer Freisetzung in die Analyse einzubeziehen einschließlich der bewussten Angriffe. Da dieser Schritt, wie schon gesagt, kaum vollständig vorgenommen werden kann, wird es einen „intuitiven, kreativen Prozess“ geben müssen, bei dem sich z.B. „Red Teams“ in regelmäßigen Abständen in die Rolle eines möglichen Angreifers hineinversetzen und (auch im Lichte neuer technologischer Entwicklungen) „Angriffsszenarien“ identifizieren. Es wird nötig sein, die als die wichtigsten anzunehmenden Szenarien für die Planung zu fixieren.

3.2 Risikomanagement

Wie oben beschrieben, können - abgeleitet aus diesen Basisinformationen - Strategien im Rahmen eines staatlichen Risikomanagements umgesetzt werden, die „unstrittig verwundbarkeitsreduzierend“ sind. Sie sollen hier noch einmal beispielhaft aus Sicht der Planung angesprochen werden.

Verhaltensänderungen der allgemeinen Bevölkerung, die im Prinzip eine Verbesserung der Sicherheitslage bewirken, können sich auf der einen Seite „unwillkürlich“ in der Gesellschaft durch „Änderung des Zeitgeistes“ als allmählicher Paradigmenwandel ergeben. Sie dürften aber nur sehr begrenzt steuerbar sein und sind in der Regel allenfalls über langfristige „Erziehungsprogramme“ beeinflussbar. Beispiele sind allerdings durchaus vorhanden, wie die ja durchaus erfolgreichen Verkehrserziehungsaktionen vor einigen Jahrzehnten („Hallo, Partner - dankeschön“, „der 7. Sinn“). In einem demokratisch legitimierten Umfeld sollten auch Überlegungen zu solchen Maßnahmen nicht mit dem Generalverdacht der „Manipulation“ von vornherein ausgeschlossen werden. Auf der anderen Seite - und hier durchaus mit einem unmittelbaren Planungsbezug - sind natürlich mögliche Verhaltensänderungen im Sinne eines höheren Sicherheitsbewusstseins in staatlichen und staatsnahen Vorsorgeeinrichtungen etwa durch Anpassung von Vorschriften und Dienstanweisungen einzuleiten (und sind natürlich auch bereits eingeleitet). Polizei und Feuerwehr und auch die Streitkräfte müssen Handlungsabläufe mit den richtigen Verhaltensweisen in Szenarien einüben, die jetzt nicht mehr ausgeschlossen werden können.

Eine mehr auf technische Anlagen gerichtete Strategie ist die **Verbesserung der inhärenten Sicherheit**, nun allerdings noch stärker in dem Sinne „idiosynchron“, dass Sicherungssysteme nicht nur durch Dummheit oder Fahrlässigkeit nicht ausgeschaltet werden können, sondern auch nicht durch aktives kriminelles Bemühen bis hin zur Einbeziehung der Bereitschaft zum Selbstmord. Im Idealfall sollte sogar der Prozess selber kein Schadenspotential haben. In die-

sem Sinne sind sicherlich alle Unfallverhütungsvorschriften und technischen Anleitungen und Anweisungen für Genehmigung und Betrieb neu zu bewerten. Auch ist eine Nachrüstung oder Neukonfiguration von Prozessen nicht auszuschließen, sowie eine Prüfung der Möglichkeit, hohe Konzentrationen lebenswichtiger Funktionen (Personal, Infrastruktur) etwa in Ämtern zu vermeiden. Es sei daran erinnert, dass auch zu Zeiten des Kalten Krieges beunruhigende Szenarien für den angriffsvorbereitenden Einsatz feindlicher Sabotagetrupps diskutiert wurden (etwa die Ausschaltung der wenigen erfahrenen Luftbildaufklärer für die Drohne CL 89).

Das Verhalten von Systemen im Schadensfall (**Schadensminimierung**) ist natürlich wie viele andere Aspekte bereits heute planerischer Alltag. Im Prinzip ergibt sich hier keine neue Situation. Allenfalls könnte Handlungsbedarf gesehen werden unter dem Blickwinkel, dass Situationen denkbar sind, in denen etwa ein Selbstmörder oder Kommandos mit einer für uns ganz unvorstellbaren Brutalität einen Schaden verursachen könnte, den man früher gänzlich als nicht vorsorgerelevant ausgeschlossen hätte.

Die Strategie der gezielten und mit großem Aufwand vorangetriebenen **Verstärkung der Asymmetrie** wird sicher auch in der Zukunft stark von den USA getragen werden, und von da an die Verbündeten heran getragen werden. Das findet in den USA dabei durchaus auch mit dem „Hintergedanken“ statt, dass auf diesem Wege gleichzeitig eine „wirtschaftlich nützliche“ Asymmetrie zwischen den USA und dem Rest der Welt gefördert wird. Auch Europa hat allerdings mit den neuen Initiativen für sicherheitsrelevante Forschung und Technologie erste Schritte vollzogen, um sich technologische Optionen, die einen Vorteil gegenüber asymmetrischen Gegnern verschaffen können, zu sichern¹¹. Auf den Aspekt einer schutzorientierten „explorativen“ Biowaffenforschung sei hier nur noch einmal hingewiesen.

Die **Steigerung des Abwehraufwandes**, die im Grunde die „einfachste“ Strategie ist, kann letztlich nur durch Geld realisiert werden. Die Gesellschaft muss deshalb unvermeidlich die Prioritäten klar benennen. Den Zielkonflikt könnte man überpointiert z.B. so formulieren: „ist eine Steigerung der Eigenbeteiligung in der Krankenversicherung hinzunehmen, wenn so die Zahl der Terrortoten auf einige Hundert pro Jahr reduziert werden kann“. Natürlich ist dieser unmittelbare Zusammenhang nicht ernst gemeint, es muss aber deutlich werden, dass diese beschränkenden Zusammenhänge nicht ignoriert werden dürfen. Tiefer gehende Entscheidungen werden sicher auf uns zukommen,

¹¹ Deutschland sollte hier die Praxis überdenken, dass beim Thema Verteidigung und Sicherheit die Forschungs-„förderung“ seit dem 2. Weltkrieg tabuisiert ist. Dies wird letztlich im Ausland nicht verstanden.

auch wenn man sie vielleicht noch einige Zeit durch Straffung, Neudefinition und -verteilung sowie (medienwirksame) Ad-hoc-Maßnahmen hinausschieben kann.

Eine begleitende **Analysebasis** ist (unpolitisch und aus wissenschaftlicher Sicht betrachtet) eine Selbstverständlichkeit (aber das hat man auch schon bei dem Instrument der Rasterfahndung geglaubt). Das gesamte Spektrum modernen Informationsmanagements (Computerlinguistik, Informationsretrieval, Mustererkennung, Vernetzung, ...) hat so hohe Bedeutung für die Effizienz des Risikomanagements, dass hier nur dringend geraten werden kann, keinen Forschungs- und Entwicklungsaufwand zu scheuen - sowohl unter zivilem als auch unter militärischem Blickwinkel.

Die für Vorsorgeinstitutionen vielleicht sogar problematischste und für einen Angreifer „risikoärmste“ und „billigste“ Möglichkeit, einer westlichen Zivilisationsgesellschaft Schaden zuzufügen, ist der vorgetäuschte Terroranschlag. Gerade unsere Wohlstandsgesellschaften haben, wie schon gesagt, eine Neigung, einen sehr hohen Sicherheitsstandard und geringe persönliche Gefährdung zu erwarten und z.B. Schadensschwellwerte im ökologischen Bereich unabhängig vom Aufwand für ihre Einhaltung sehr niedrig anzusetzen. Hinzu kommt die Erwartung, dass dies durch staatliche Organe sichergestellt werden muss. Zumindest bis zum Eintreten von „Ermüdung“ bei häufigen Fehlalarmen wird jedes Mal großer Aufwand getrieben. Es ist zu erwarten, dass diese „Angriffsvariante“ größere Bedeutung erlangen wird und es ist grundsätzlich nicht auszuschließen, dass ein „Klima der Verwundbarkeit“ entsteht, das immer wieder durch reale und vorgetäuschte Angriffe erneuert wird. Auch wenn zu hoffen¹² ist, dass eine solche Erzwingung eines ganz allgemeinen volkswirtschaftlichen Schadens für mögliche „ernsthafte“ Angreifer nicht spektakulär und spezifisch genug ist, um wirklich systematisch und strategisch genutzt zu werden, muss man immer wieder mit „unprofessionellen“ Nachahmungstätern, Psychopathen aber auch mit kriminellen Erpressern rechnen. Die jüngsten Erfahrungen mit der Erpressung des französischen Staates legen übrigens nahe, dass über eine neue (bzw. „reaktivierte“) Medienethik nachgedacht wird.

¹² Aber das ist wirklich nur eine Hoffnung.

4 Zusammenfassung

Ein sicherer Schutz gegen alle Angriffsoptionen und ihre Folgen ist ohne Aufgabe des grundlegenden kulturellen Paradigmas wohl nicht möglich. Es muss eben auch mit Angreifern gerechnet werden, die sich auf ein drastisch anderes Wertesystem berufen mit der Folge unerwarteter Verhaltensweisen, wie etwa die Durchführung von Aktionen mit einer für westliche Maßstäbe völlig irrationalen Brutalität. Hinzu kommt die bereits angesprochene grundsätzliche Asymmetrie, die sich daraus ergibt, dass der tatsächlich „ausführende Gegner“ nicht wirklich präsent ist und viel schwerer in seinen Handlungen auf Anzeichen eines Angriffes überwacht werden kann, als in der Vergangenheit ein feindlicher Staat. Das bedeutet für „den Verteidiger“, dass er im Prinzip „die gesamte Grenze“ (im übertragenen Sinne) überwachen muss, ohne zu wissen, an welcher Stelle der Angriff tatsächlich erfolgt. Bedeutete dies schon in der Vergangenheit einen prinzipiellen Angreifervorteil („Angriff ist die beste Verteidigung“), der aber durchaus nicht entscheidend sein musste, dürfte sich dieser Vorteil heute als so dominant erweisen, dass Sicherheitskonzepte unvermeidliche Restrisiken einkalkulieren müssen.

Eine „klassische Risikoanalyse“, wie sie eine rationale, naturwissenschaftlich-technische ausgerichtete Vorstellungswelt nahe legen könnte, ist für die heute gegebene Lage nur in wenigen Teilbereichen geeignet, Handlungsempfehlungen für konkretes Risikomanagement und die Planung zu begründen. Die neuen Bedrohungen stellen für den Verteidiger (durchaus nicht für den Angreifer) ein irrationales Element dar, mit dem eine notwendig rationale Planung nur schwer umgehen kann. Die letztlich verbleibende Strategie kann deshalb nur darin bestehen, durch ein allgemeines „Verwundbarkeitsmanagement“ die Gesellschaft so „robust“ wie möglich zu machen, möglichst unabhängig von einzelnen Annahmen oder tatsächlich eintretenden Schadensereignissen. Daraus ergibt sich Handlungsbedarf für alle Vorsorgeeinrichtungen und die staatliche Planung.

Grundsätzlich wird es notwendig sein, dass die (westlich ausgerichtete) Gesellschaft die terroristische Bedrohung ihrer Sicherheit als ein nicht völlig auszuschließendes „Allgemeinrisiko“ wahrzunehmen lernt, ähnlich wie den Straßenverkehr oder die „zufälligen“ Unfälle. Wir werden uns deshalb zum Terrorismus und seiner Bekämpfung an Bilanzen und Rechenschaftsberichte der Regierung, an Aufklärungsprogramme und einen unterschweligen „vorsorglichen“ Aktivitätspegel in den staatlichen und staatsnahen Vorsorgeinstitutionen gewöhnen müssen. Besonders sensitiv dürfte dabei die politische Frage sein, welchen (finanziellen) Aufwand man für die Verbesserung der Sicherheitslage treiben will, d.h. letztlich, wie viele Terrortote man für „hinnehmbar“ hält.

Vor allem muss der Bevölkerung klar sein (oder gemacht werden), dass nicht jedes „Tagesereignis“, so schrecklich es sein mag, ad-hoc zu einem hektischen Eingriff in langfristig stabil zu haltende Strukturen führen darf, der die notwendige „Wohldurchdachtheit und Rationalität“ des Vorsorgesystems untergräbt. Genau dieses zu erreichen, ist letztlich Ziel der terroristischen Angriffe.

Weitere Themen in dieser Reihe sind erschienen oder in Vorbereitung

Stand April 2009:

Hochtechnologien in der Wehrtechnik
Mai 2004

Betrachtungen zum Risikobegriff vor dem Hintergrund naturwissenschaftlich-technischer Entwicklungen und staatlicher Planung und Vorsorge
August 2004

Langfristige Technologieentwicklungen
Anmerkungen zu Arbeitswelt, Rationalisierung und Ausbildung
Januar 2005

Zur Entstehungsgeschichte der modernen Technik
März 2006

Disruptive Technologies - widening the scope -
April 2006

Betrachtungen zur äußeren und inneren Sicherheit
Gedanken zu einer „Robusten Gesellschaft“
August 2006

Utopien und Planung
- der steinige Weg zur Wirklichkeit -
November 2006

Prognosen, Utopien, Planung und staatliches Handeln
Gedanken zum Diskurs „Technik und gesellschaftlicher Wandel“
April 2008

Zum Komplexitätsproblem in Entscheidungsprozessen
November 2008

