CRN REPORT

Factsheet

Identifikation von Risiken

Zürich, Juli 2009

Crisis and Risk Network (CRN)
Center for Security Studies (CSS), ETH Zürich

Im Auftrag des Bundesamtes für Bevölkerungsschutz (BABS)

CRN
Supported by ISN

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Autor: Beat Habegger

Kontakt:
Center for Security Studies
Seilergraben 45–49
ETH Zürich
CH-8092 Zürich
Schweiz
Tel.: +41-44-632 40 25

crn@sipo.gess.ethz.ch
www.crn.ethz.ch

Auftraggeber: Bundesamt für Bevölkerungsschutz (BABS)
Projektaufsicht BABS: Stefan Brem, Chef Risikogrundlagen und Forschungskoordination
Auftragnehmerin: Center for Security Studies (CSS) der ETH Zürich
Projektleitung ETH-CSS: Myriam Dunn Cavelty, Head New Risks Research Unit; Andreas Wenger, Director CSS; Victor Mauer, Deputy Director CSS

INHALTSVERZEICHNIS

ABSTRACT

Dieses Factsheet bietet eine Einführung in einige grundlegende Aspekte der Risikoidentifikation. Dabei handelt es sich um die erste Phase eines integrierten Risikomanagements, die nachfolgend durch die Risikobewertung und die Risikominderung zu ergänzen ist. Das Factsheet ist folgendermassen aufgebaut: Es zeigt einleitend anhand konkreter Fälle, mit welchen Herausforderungen Politik, Wirtschaft und Gesellschaft in der Vergangenheit konfrontiert waren. Anschliessend werden verschiedene konzeptionelle Aspekte beleuchtet und voneinander abgegrenzt. Schliesslich zeigen Beispiele aus Staat und Unternehmen, welche Massnahmen in der Praxis unternommen werden. Im Anhang werden in Kurzform einige einfache und in standardisierter Weise aufbereitete Instrumente zur Risikoidentifikation vorgestellt.

1. AUSGANGSLAGE

Im Nachhinein ist man immer schlauer und meistens ist es einfach, die Zeichen zu erkennen, die eigentlich schon lange auf kommende Unbill hingedeutet haben. Viele Krisen und Katastrophen der Vergangenheit ereigneten sich nicht aus heiterem Himmel. Manche hätten sich wohl vermeiden lassen, wenn die ersten Signale erkannt worden wären und – noch wichtiger – die Verantwortlichen darauf reagiert hätten. Ein Blick zurück zeigt zahlreiche Beispiele dafür. So hat etwa die European Environment Agency in ihrem Bericht «Late Lessons of Early Warnings» 14 Fallstudien publiziert, die sich alle mit zunächst unterschätzten Gefahren für die Gesundheit von Menschen und die Umwelt beschäftigen. Viele der teilweise drastischen Konsequenzen wären oft wesentlich weniger schlimm gewesen, wenn die Warnungen erkannt und ernst genommen worden wären.[1] Nachfolgend soll anhand drei exemplarischer Fälle – Asbest, Finanzkrise und Tsunami – die Bedeutung einer frühzeitigen Identifikation von Risiken aufgezeigt werden.

Ein bekanntes, wenn auch kontrovers beurteiltes Beispiel für die lange Zeitspanne, die zwischen ersten Warnungen und konkretem Handeln liegen kann, sind die unterschätzten Gefahren, die vom Bau- und Isoliermaterial *Asbest* ausgehen.[2] Bereits 1898 wies die britische Fabrikinspektorin Lucy Deane auf die schädlichen Wirkungen von Asbeststaub hin. Sie schrieb in einem ihrer Berichte:[3]

> The evil effects of asbestos dust have also instigated a microscopic examination of the mineral dust by HM Medical Inspector. Clearly revealed was the sharp glass-like jagged nature of the particles, and where they are allowed to rise and to remain suspended in the air of the room in any quantity, the effects have been found to be injurious as might have been expected.

Andere Fabrikinspektorinnen kamen in der Folge zu ähnlichen Schlüssen und 1906 wurden auch in einem französischen Bericht 50 Todesfälle von Arbeiterinnen mit Asbest in Verbindung gebracht. Diesen Beobachtungen durch medizinische Laien wurde aber kaum Beachtung geschenkt und selbst frühe wissenschaftliche Gutachten vermochten keine Schutzmassnahmen auszulösen. In den folgenden Jahrzehnten gab es immer wieder Hinweise und auch wachsende wissenschaftliche Evidenz für die durch Asbest verursachten Gesundheitsrisiken. Aus vielerlei Gründen wurden diese jedoch von den Behörden lange ignoriert bzw. es wurden nur nach und nach Einschränkungen hinsichtlich des Einsatzes und der Anwendung von asbesthaltigen Materialien vorgenommen.

Mehr als hundert Jahre nach den ersten Beobachtungen einer britischen Fabrikinspektorin untersagte schliesslich die Europäische Union (EU) im Jahre 1998 den Gebrauch von Asbest vollständig. In vielen Schwellen- und Entwicklungsländern jedoch, aber etwa auch in Kanada als einem der wichtigsten Förderländer, wird Asbest weiterhin produziert und eingesetzt. Eine Schätzung aus dem Jahre 1999 geht davon aus, dass in der EU in den folgenden 35 Jahren 250'000 bis 400'000 Todesfälle durch Asbestexposition (mit-)verursacht werden; ein Bericht der Neuen Zürcher Zeitung nennt gar die Zahl von bis zu 500'000 mit Asbest assoziierten Todesfällen in den nächsten 30 Jahren.[4] Für manche Unternehmen hatten die unterschätzten Risiken fatale Folgen. Firmen, die asbesthaltige Produkte herstellten, wurden

1 European Environmental Agency, *Late Lessons from Early Warnings: The Precautionary Principle 1896–2000* (Environmental Issue Report No. 22, Copenhagen, 2001).

2 Siehe zum Folgenden David Gee and Morris Greenberg, «*Asbestos: from 'magic' to malevolent mineral*», in: *European Environmental Agency, Late Lessons from Early Warnings: The Precautionary Principle 1896–2000* (Environmental Issue Report No. 22, Copenhagen, 2001), S. 52-63.

3 Ibid., S. 52.

4 Bittere Lehren im Westen – Zweckoptimismus in Schwellenländern, *Neue Zürcher Zeitung*, 29. August 2008, S. 58.

auf hohe Schadenersatzsummen verklagt: Allein in den USA belaufen sich die entsprechenden Zahlungen auf 200 Milliarden Dollar, wovon Versicherer 60 Prozent und die betroffenen Firmen den Rest trugen. Dutzende von Firmen wurden durch Sammelklagen in den Konkurs getrieben und allein die ABB hat beispielsweise über 2 Milliarden US Dollar an Entschädigungen bezahlt.[5]

Auch in der jüngsten Gegenwart finden sich Beispiele dafür, dass warnende Stimmen auf wachsende Risiken hinwiesen ohne damit angemessene Beachtung zu finden. Ein interessanter Fall ist die ab 2007 von den USA ausgehende *Finanzkrise*. Diese begann in einem Teilsegment des amerikanischen Kreditgeschäfts – den so genannten «subprime loans» des amerikanischen Immobilien- und Hypothekarmarkts – und hat sich sowohl geographisch wie auch sektoriell immer mehr ausgeweitet und letztlich die gesamte Weltwirtschaft in eine kritische Situation gebracht. Zahlreiche Finanzinstitute mussten derart gigantische Abschreibungen vornehmen, dass sie kollabierten oder nur mittels Staatshilfen überleben konnten. Die Kapital- und Aktienmärkte wurden in einen fatalen Abwärtssog gezogen und Liquiditätsengpässe, Kreditverknappungen und ein gravierender Vertrauensverlust seitens der Investoren führten letztlich zu einer – bis heute anhaltenden – massiven Rezession, einschliesslich den damit verbunden Arbeitsplatzverlusten. Es ist ein Leichtes zu behaupten, diese Krise sei absehbar gewesen – wie es derzeit natürlich viele tun. Tatsache ist, dass die meisten Experten die Risiken in diesem Ausmass nicht erkannt oder zumindest massiv unterschätzt haben. Es ist ebenso klar, dass es durchaus warnende Stimmen gab. Ein prominentes Beispiel ist etwa die britische Zeitschrift «The Economist», die bereits 2003 auf die mit der Verbriefung von Kreditrisiken verbundenen Gefahren hingewiesen und die ungenügende Regulierung dieses Markts kritisiert hat.[6] Auch andere haben vor den Folgen der Entwicklungen auf den Kapitalmärkten gewarnt; letztlich gelang es ihnen jedoch nicht, ihre Kritik so vorzutragen, dass die wirtschaftlichen Verwerfungen der letzten zwei Jahre hätten vermieden werden können.

Ein drittes Beispiel dafür, wie zentral die rechtzeitige Identifikation von Risiken sein kann, ist die Katastrophe, die ein *Tsunami* im Indischen Ozean im Dezember 2004 anrichtete. Tsunamis sind heftige Meereswellen, die meistens durch Erdbeben auf dem Meeresgrund verursacht werden und beim Auftreffen auf dem Festland schwere Verwüstungen anrichten können. Im Pazifischen Ozean gibt es seit vielen Jahren bewährte Tsunami-Frühwarnsysteme und in stark erd- und seebebengefährdeten Staaten wie etwa Japan wurden neben der Frühwarnung auch viele bauliche Schutzmassnahmen getroffen. Im Indischen Ozean hingegen haben wirksame Frühwarnsysteme bisher gefehlt. Deshalb konnte der Tsunami vom 26. Dezember 2004 derart gewaltige Schäden anrichten. Das Seebeben vor der indonesischen Insel Sumatra erreichte auf der Richterskala eine Magnitude von 9,3 (eines der stärksten je gemessenen Beben) und kostete rund 230'000 Menschen das Leben. Mehr als die Hälfte davon – geschätzte 140'000 Menschen – traf es in Indonesien. Obwohl Indonesien von Vulkanen umgeben ist und aufgrund seiner tektonischen Lage als stark erdbebengefährdet gilt, gab es bis dahin kein wirksames Tsunami-Frühwarnsystem. Dieser Mangel wurde seither behoben und das neue System hat sich bereits bewährt: Ohne bereits voll einsatzfähig zu sein, warnte es am 17. September 2007 rechtzeitig vor einem Beben der Stärke 8,4, so dass die indonesischen Behörden eine Tsunamiwar-

5 Ibid.

6 The Economist, *Who's Carrying the Can?* (Special Report: Bank Lending), *The Economist*, 14 August 2003.

nung 15-20 Minuten vor dem Auftreffen der Welle auf dem Festland ausgeben konnten.[7]

Diese drei Beispiele illustrieren die Bedeutung einer rechtzeitigen Identifikation von Risiken und entsprechenden Massnahmen zur Frühwarnung. Sie zeigen, dass sich menschliches Leid und wirtschaftliche Schäden vermeiden lassen, wenn Signale rechtzeitig erkannt und aufgenommen werden. Die Beispiele geben aber auch einen Hinweis darauf, dass beim Erkennen und Einordnen von Warnungen ein feines Gleichgewicht zwischen übertriebener Vorsicht, überstürztem Handeln und eigentlicher Paralyse zu wahren ist. Insgesamt zeigen die Beispiele, dass der Risikoidentifikation im Rahmen eines umfassenden Risikomanagements grosse praktische Bedeutung zukommt.

7 International Risk Governance Council (2009), *Risk Governance Deficits (Policy Report)* (Geneva: IRGC, 2009), S. 14

2. KONZEPTIONELLE ASPEKTE DER RISIKOIDENTIFIKATION

In diesem Kapitel werden die folgenden konzeptionellen Aspekte der Risikoidentifikation beleuchtet: Scanning ist von der Frühwarnung abzugrenzen (2.1); sowohl fehlende Warnungen wie auch Fehlalarme sind zu vermeiden (2.2); strategische Überraschungen stellen besondere Herausforderungen (2.3); Kreativität, Urteilsvermögen und der geschickte Einsatz von Technologie ermöglichen ein besseres Erkennen von Risiken (2.4).

2.1 Scanning und Frühwarnung

Die erste Aufgabe im Rahmen der Risikoidentifikation ist ein umfassendes *Scanning* der sozialen, technologischen, wirtschaftlichen, ökologischen und politischen Umwelt. Ziel ist es zunächst, den «strategischen Radar»[8] so breit wie möglich aufzuspannen, um möglichst keine Risiken unerkannt zu lassen. Dieses «Environmental Scanning»[9] erstreckt sich primär auf das Entdecken von noch unerkannten oder neu entstehenden Risiken, oder solchen, die zwar erkannt sind, jedoch in einem neuen oder ungewohnten Kontext auftreten («emerging risks»). Zudem werden diese Risiken zwar vielfach als bedeutsam wahrgenommen, oft ist aber noch unklar, was sie auszeichnet und wie sie sich entwickeln könnten, weshalb sich keine bestimmten präventiven Massnahmen unmittelbar anbieten. Oft entwickeln sie sich nur langsam und über lange Zeit aus allgemeinen Trends und Entwicklungen – etwa dem technologischen Fortschritt – heraus. Beim Asbest beispielsweise lag die Aufmerksamkeit auf den hervorragenden Eigenschaften dieses Materials: Es ist extrem hitzebeständig, resistent gegen viele Chemikalien und gleichzeitig thermisch und elektrisch sehr gut isolierend.[10] Die negativen Konsequenzen hingegen wurden lange weitgehend übersehen oder gar bewusst ausgeblendet. Deshalb sind potenzielle Risiken und ihre möglichen Entwicklungspfade kontinuierlich zu überwachen (Monitoring), um sich abzeichnende Veränderungen möglichst frühzeitig zu erkennen.

Ausgehend von den gesammelten Informationen über neu auftretende Risiken lässt sich eine wirksame *Frühwarnung* aufbauen. Diese sucht nach Ereignissen und Entwicklungen, die auf Veränderungen und Trendbrüche in einem Umfeld hinweisen, das bis dahin als stabil und wenig wandelbar galt.[11] Damit lassen sich Überraschungseffekte vermeiden, die dazu führen, dass Risiken zu realen Gefahren werden und Ziele, Interessen und Werthaltungen von Organisationen oder der Gesellschaft insgesamt bedrohen. Die Entscheidungsträger sollen genügend Zeit erhalten, um rechtzeitig Gegenmassnahmen einzuleiten, Schäden zu verhindern und die potenziellen sozialen und wirtschaftlichen Kosten möglichst tief zu halten. Die zentrale Idee der Frühwarnung besteht darin, dass Veränderungen und Trendbrüche selten unvermittelt auftreten, sondern sich durch zeitlich vorauslaufende Signale bzw. Indikatoren, die nicht leicht zu erkennen und zu deuten sind, ankündigen. Solche «schwachen Signale» zeigen sich oft lange bevor Experten und Entscheidungsträger in Wirtschaft und Gesellschaft auf Trendbrüche und daraus neu entstehende Risiken aufmerksam werden; basierend auf blosser Intuition und parallel zum Tagesgeschäft lassen sie sich nicht erkennen.[12] Deshalb braucht es neben einer interdis-

8 Krystek, Ulrich und Günter Müller-Stewens, «Strategische Frühaufklärung» in: Dietger Hahn und Bernard Taylor (Hrsg.), *Strategische Unternehmensplanung – Strategische Unternehmensführung* (Heidelberg: Physica, 8. Auflage, 1999), S. 501.

9 Siehe etwa Chun Wei Choo, *Information Management for the Intelligent Organization: The Art of Scanning the Environment* (Medford: Information Today, 2002).

10 Bittere Lehren im Westen, *Neue Zürcher Zeitung*, S. 58.

11 Krystek und Müller-Stewens, S. 501-6.

12 Habegger, Beat, «Risk Analysis and Management in a Dynamic Risk Landscape», in: Beat Habegger (ed.), *International Handbook on Risk Analysis and Management* (Zurich: Center for Security Studies ETH Zurich, 2008), S. 13-32, hier S. 21-23.

ziplinären und sektorübergreifenden Perspektive, die bewusst auch Leute jenseits des Mainstreams einbezieht, ein professionelles Frühwarnsystem.

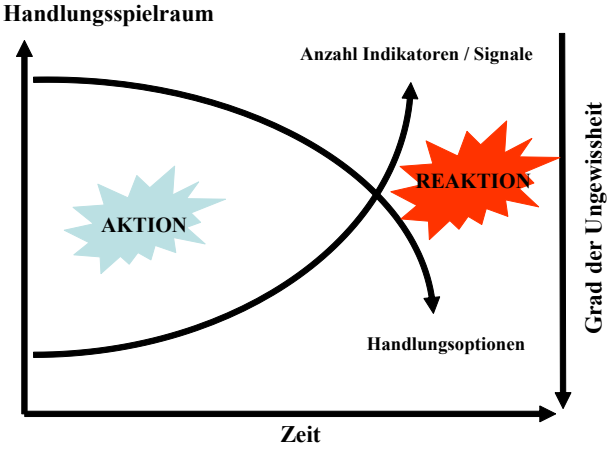

Abbildung 1: Konzept der Frühwarnung

Frühwarnsysteme bilden das institutionelle Rückgrat, um diese schwachen Signale aufzufangen. Sie sollen Informationen so lange akkumulieren bis offensichtlich wird, dass ein neues Risiko sich formiert und potenziell zu einer Bedrohung werden kann. Grundsätzlich gilt die Vermutung, dass das Sammeln von mehr Informationen zu mehr Hinweisen auf mögliche Umweltveränderungen führt. Moderne Informations- und Kommunikationstechnologien machen Informationen immer leichter zugänglich und verfügbar. Andererseits ist paradoxerweise festzustellen, dass die grosse Menge verfügbarer Informationen es zugleich schwieriger macht, die wirklich wichtigen, d.h. auf kommende Risiken hindeutenden Signale herauszufiltern. Informationen zu technologischen, wirtschaftlichen, kulturellen oder politischen Trends werden aus einer Vielzahl von Quellen gespiesen – wissenschaftliche Zeitschriften und Konferenzen, Medien aller Art, Internet und Datenbanken, persönliche und institutionelle Netzwerke, etc. Damit lässt sich verhindern, dass Analysten ihre Informationen einseitig auswählen und nur berücksichtigen, was sie in ihren Überzeugungen bestätigt. Idealerweise sind deshalb auch bewusst Querdenker einzubeziehen, die Informationen auf kreative Weise interpretieren.

Frühwarnsysteme können formal ausgestaltet sein und auf automatisch generierte Informationen reagieren – wie etwa bei epidemiologischen Daten im Vorfeld einer Pandemie – oder sie können informell sein und sich auf menschliches Urteilsvermögen abstützen – wie etwa im Fall der auf die Asbestgefahren aufmerksam gewordenen Fabrikinspektoren. Sie speichern in der Regel die gesammelten Informationen und bereiten sie überdies in einer mehr oder weniger standardisierten Form so auf, dass sie nachfolgend als Entscheidungsgrundlage dienen können.

2.2 Fehlende Warnungen und Fehlalarme

Wären Frühwarnsysteme perfekt (und vorausgesetzt, die Verantwortungsträger nehmen die Warnungen ernst und setzen sie in entsprechendes Handeln um), dann könnten sie viel Unheil abwenden, ohne je einen falschen Alarm auszulösen.[13] Leider trifft dies in der Realität nicht zu: Manchmal fehlen Warnungen, obwohl eine Gefahr besteht (so genannte «false negatives»); manchmal weisen Signale auf eine Gefahr hin, die es in Wahrheit gar nicht gibt (so genannte «false positives»).

Die aus Fehlern resultierenden Kosten können sowohl in menschlicher wie wirtschaftlicher Hinsicht sehr hoch sei. Wenn Risiken entstehen, weil die ersten Signale nicht erkannt werden und sie deshalb nicht umfassend beurteilt und präventiv gemindert werden: bei Asbest, Tsunami und Finanzkrise hätten sich so hohe Schäden verhindern lassen. Aber auch Fehlalarme sind kostspielig: Zum einen können sie zu Aktionismus führen und beispielsweise durch ungerechtfertigte oder übertriebene Regulierungen tech-

13 International Risk Governance Council, S. 12.

nologische Innovationen verhindern und damit unternehmerische Initiativen hemmen; Zum anderen werden knappe Ressourcen zur Risikoprävention und zur Minderung von Schäden möglicherweise falsch zugeteilt.

Wiederholte Fehlalarme mindern das Vertrauen der Öffentlichkeit in die Zuverlässigkeit der Warnsysteme und führen dazu, dass diese bei einem wirklichen Ernstfall nicht mehr beachtet werden.[14] Ein wichtiger Faktor ist dabei die Qualität der verfügbaren Informationen. Wenn zu wenig und erst noch lücken- oder fehlerhafte Daten und Fakten vorliegen, werden Risiken zum einen möglicherweise gar nicht erst erkannt; zum andern besteht vermutlich zu wenig Vertrauen in die Zuverlässigkeit der erhobenen Informationen, um wirklich entsprechende Warnungen auszusprechen. Pardoxerweise kann sich aber nicht nur dieser Mangel an Informationen, sondern auch deren Überfluss negativ auf die Zuverlässigkeit der Frühwarnung auswirken, wenn eine Fülle von Informationen zu einem Mangel an wirklicher Aufmerksamkeit führt.[15] Die Herausforderung besteht somit auch darin, in einer informationsgesättigten Umgebung die wirklich wichtigen Signale herauszufiltern und die knapp gewordene Ressource der Aufmerksamkeit auf diese zu lenken.[16]

Letztlich besteht die Herausforderung einer wirksamen Frühwarnung somit darin, ein feines Gleichgewicht zu halten zwischen dem rechtzeitigen Reagieren auf erste Signale und einer gewissen Vorsicht zur Vermeidung von regulatorischem Aktivismus und wachsender Gleichgültigkeit seitens der Gesellschaft.

2.3 Strategische Überraschungen

Jenseits der Risiken, die sich in einem systematischen, durch menschliches Urteilsvermögen und technologische Hilfsmittel unterstützten Prozess der Risikoidentifikation entdecken lassen, kann es zu eigentlichen strategischen Überraschungen kommen. Dabei handelt es sich um Ereignisse, die derart weit entfernt sind von den historischen Erfahrungen und den Erwartungen, die sich für die allermeisten Beobachter aus der Analyse von Vergangenheit und Gegenwart sowie ihrer Projektion in die Zukunft ergeben, dass sie bis zu ihrem Auftreten schlicht unerkannt bleiben.

In seinem Bestseller «The Black Swan» argumentiert Nassim Nicholas Taleb, dass die wichtigsten Ereignisse auf der Welt selten sind, extreme Wirkungen entfalten und weder statistisch noch mit anderen Hilfsmitteln vorhersehbar sind.[17] Gleichwohl stützen sich die Menschen bei der Planung und Vorhersage künftiger Ereignisse in der Regel auf früher gemachte Erfahrungen. Sie ziehen ihre Schlüsse aufgrund dessen, was gut bekannt, mess- und damit modellierbar ist und geben sich deshalb gerne der Illusion hin, alles unter Kontrolle zu haben. Sind sind gewohnt, Risiken und Wahrscheinlichkeiten (im stochastischen Sinn) als normalverteilt anzusehen und deshalb davon auszugehen, dass katastrophale Ereignisse äusserst selten eintreten. Taleb meint, dass solche unerwarteten Dinge viel häufiger eintreten als die statistischen Modelle erwarten liessen. Er nennt diese Ereignisse «schwarze Schwäne» in Anlehnung an die ersten Europäer, die in Australien ankamen und die vermeint-

14 Ibid.

15 Nye, Joseph S., *The Paradox of American Power* (Oxford: Oxford University Press, 2002), S. 43.

16 Habegger, Beat, Chris Pallaris, und Vivian Fritschi, *Emerging Threats in the 21st Century; Seminar 1: The Changing Threat Environment and Its Implications for Strategic Warning* (Zurich: Center for Security Studies, ETH Zurich, 2006), S. 8.

17 Taleb, Nassim Nicholas, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007).

liche Tatsache, dass Schwäne immer weiss seien, gründlich revidieren mussten.

Schwarze Schwäne sprengen konventionelle Denkmuster und laufen unseren Vorstellungen bezüglich dessen, was «realistischerweise» zu erwarten ist, entgegen. In einer Welt, die von rationalistischem Denken in Normalverteilungen geprägt ist, bilden sie eigentliche Anomalien. In die Sprache der Stochastik übersetzt bilden sie den so genannten «Fat Tail»[18] am eigentlich «dünnen» Ende normalverteilter Ereignisse: sie weisen darauf hin, dass katastrophale Ereignisse wahrscheinlicher sein könnten, als wir anzunehmen pflegen. Schwarze Schwäne lehren uns, den auf Rationalität fundierenden Modellen, Strukturen und Gewissheiten zu misstrauen. Oft sind sie nützlich und sinnvoll. Zuweilen kommt es aber ganz anders als angenommen. Gerade deshalb verlangt die Risikoidentifikation auch nach Kreativität und menschlicher Intuition.

Die kritischen Wendepunkte in der Geschichte waren häufig schwarze Schwäne. Taleb nennt etwa die Verbreitung von Christentum und Islam, den Ersten Weltkrieg, oder die Terroranschläge auf die USA vom 11. September 2001.[19] Bei letzteren bestand die eigentliche Überraschung nicht im Anschlag als solchem. Schliesslich hatte es bereits zuvor Angriffe auf das World Trade Center in New York City sowie Einrichtungen amerikanischer Bundesbehörden (etwa beim Bombenanschlag in Oklahoma City 1995) gegeben. Im Nachhinein ergaben auch die Untersuchungen der 9/11-Commission, dass im Sommer 2001 etliche nachrichtendienstliche Hinweise auf Vorbereitungshandlungen terroristischer Gruppen eingingen. Die damalige Nationale Sicherheitsberaterin Condoleezza Rice erklärte sogar, dass die Nachrichtendienste ziemlich spektakuläre Aussagen zu in der nahen Zukunft bevorstehenden Angriffen gemacht hätten, allerdings seien die daraus resultierenden Schlussfolgerungen auf frustrierende Weise «vage» gewesen.[20] Das Besondere an 9/11 war letztlich nicht der Angriff als solcher, sondern die Form seiner Ausführung, die in dieser Form kaum vorhersehbar war. Niemand hatte damit gerechnet, dass Flugzeuge als Tatwaffen eingesetzt werden könnten. Konventionelles Denken ging davon aus, dass eine Bombe ins Flugzeug geschmuggelt wird und Geiseln genommen werden mit dem Ziel, irgendwelche Leistungen (z. Bsp. die Freilassung politischer Gefangener) zu erpressen. Dass das Flugzeug selber als Waffe genutzt werden könnte und dass die Attentäter nichts anderes suchen als Tod und Zerstörung (einschliesslich ihrer selbst) passte nicht in die Denkschemen der Nachrichtendienste.[21]

2.4 Fähigkeiten zum Aufspüren von Risiken

Das Aufspüren von Risiken verlangt mindestens drei grundlegende Fähigkeiten: Kreativität, Urteilsvermögen und technologische Hilfsmittel. Wenn Risiken

18 Bremmer, Ian and Preston Keat, *The Fat Tail: The Power of Political Knowledge for Strategic Investing* (Oxford: Oxford University Press, 2009).

19 Im Übrigen sieht Taleb auch in der gegenwärtigen Finanz- und Wirtschaftskrise einen «schwarzen Schwan», wie er einem Artikel in der Financial Times erläuterte. Dort nennt er auch 10 Prinzipien, wie die Welt sich resistenter machen könnte gegen künftige ähnliche Ereignisse. Siehe Nassim Nicholas Taleb, «*Ten principles for a Black Swan-proof world*», *Financial Times*, 7 April 2009.

20 Rice, Condoleeza (2004). Opening Remarks: The National Commission on Terrorist Attacks upon the United States. Washington D.C., April 8, 2004, S. 6.

21 Die Möglichkeit einer Flugzeugentführung durch einen Selbstmordattentäter («suicide hijacking») wurde zwar durch die Flugaufsichtsbehörden beiläufig erörtert, jedoch konnten sie keine konkreten Hinweise für entsprechende Pläne finden und haben diese Option bei den Security Briefings für die Fluggesellschaften auch nicht erwähnt. Siehe *The 9/11-Commission-Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington D.C.: U.S. Government Printing Office), S. 264. Tom Clancy hat in seinem Politthriller Debt of Honour (1994) ein ähnliches Szenario beschrieben.

neu sind, braucht es die Fähigkeit, sich Auftreten und Verbreitung überhaupt vorzustellen. Gerade strategische Überraschungen verlangen besonders nach Kreativität. Offensichtlich sind viele Menschen nur beschränkt in der Lage, entsprechendes kreatives Potenzial freizusetzen und dem menschlichen Denken inhärente kognitive Grenzen zu überwinden. Meistens besitzen weder Experten, die nach Risiken suchen und sie bewerten, noch Entscheidungsträger, die eigentlich für die strategische Politikformulierung zuständig wären, die dafür notwendigen Fähigkeiten und zeitlichen Ressourcen. Wie gesagt: im Nachhinein finden sich immer Stimmen, die vor einem eingetretenen Ereignis schon lange gewarnt haben wollen und natürlich finden sich immer warnende, aber nicht wahrgenommene Stimmen. Häufig sind aber auch die notorischen Kassandren, die regelrecht darauf warten, dass der von ihnen beschworene Worst Case eintritt, um sich damit hinterher in der öffentlichen Meinung zu profilieren. Obwohl dieses Vorgehen sicher nicht der Normalfall – und natürlich alles andere als hilfreich – ist, lässt sich daran trefflich illustrieren, wie schmal der Grat zwischen kreativem Denken und abstrusen Gedankenspielereien häufig ist, und wie anspruchsvoll es ist, im jeweiligen Einzelfall die richtigen Schlüsse zu ziehen.

Deshalb braucht es, zweitens, ein ausgeprägtes Urteilsvermögen, um realistisch abzuschätzen, ob neu entstehende Risiken zu eigentlichen Gefahren erwachsen könnten und wie bedrohlich dies wäre, ohne gleich auf jedes mögliche Signal mit übertriebener Vorsicht zu reagieren. In der Sicherheitspolitik beispielsweise sind die Verantwortungsträger ständig konfrontiert mit einer Vielzahl von hypothetischen Bedrohungen und Verwundbarkeiten. Solche Szenarien werden aus zahlreichen Quellen gewonnen: dem institutionalisierten Prozess der Risikoidentifikation durch die Nachrichtendienste oder anderer Behörden, dem bewussten Nutzen des kreativen Potenzials der Gesellschaft oder dem gezielten Ausspionieren von Urhebern möglicher terroristischer Angriffe. Offensichtlich kann aber nicht auf alle potenziell möglichen Szenarien reagiert werden.[22] Das Aktionsspektrum reicht letztlich von einem «hypervorsichtigen Ansatz» zu einem eigentlichen «Laissez-faire-Ansatz»: Ersterer sieht für jede mögliche Bedrohung massgeschneiderte präventive Massnahmen sowie die Planung für den Ernstfall vor. Letzterer hingegen verzichtet angesichts der Ungewissheit bezüglich dessen, wie eine künftige Bedrohung sich konkret manifestieren könnte, auf jegliche Massnahmen, die auf einen spezifischen Fall zugeschnitten sind und fokussiert sämtliche Anstrengungen auf die übergeordneten sicherheitsstrategischen Vorgaben. Es ist offensichtlich, dass ein angemessenes Vorgehen irgendwo in der Mitte des aufgespannten Spektrums zu suchen ist. Welche konkreten Ansätze zur Entwicklung eines sinnvollen Vorgehens möglich sind, wird an anderer Stelle noch ausführlicher zu beleuchten sein. Grundsätzlich lässt sich aber festhalten, dass die Gefahr von Entwicklungen, die schwer wiegende Folgen haben könnten, tendenziell eher heruntergespielt oder gar gänzlich ignoriert werden. Gründe dafür sind etwa das Vermeiden von «kognitiven Dissonanzen» oder die schlichte Weigerung, den gewohnten (und durchaus erfolgreichen) bisherigen Gang der Dinge zu stören. So lassen sich unangenehme Entscheidungen vermeiden, für die keine passenden Lösungen bereit stehen.

Obwohl dem Mensch im Prozess der Risikoidentifikation zweifellos die Schlüsselrolle zukommt, reichen seine Kreativität und sein Urteilsvermögen allein zuweilen nicht aus. Deshalb werden, drittens, auch

22 Jackson, Brian A. and David R. Frelinger, *Emerging Threats and Security Planning: How Should We Decide What Hypothetical Threats to Worry About? (Occasional Paper)*, Santa Monica: RAND Corporation, 2009, S. 4-5.

technologische Hilfsmittel eingesetzt. Diese können einerseits kreative Prozesse unterstützen (etwa im Bereich von Internet und Datenbanken) und andererseits schwache Signale, die dem menschlichen Beobachter verborgen bleiben (beispielsweise Erdbebendetektoren), selber aufgreifen. Den Einsatz von technologischen Mitteln besonders stark forciert hat die Regierung Singapurs (siehe auch Kapitel 3.2). Ihr «Risk Assessment and Horizon Scanning»-System (RAHS) experimentiert mit einer Vielzahl von teilweisen komplexen Technologien zur verbesserten Suche nach Informationen sowie ihrer Strukturierung und Visualisierung. Manche Anwendungen – wie etwa bestimmte Komplexitätsanalysen – wurden sogar eigens dafür entwickelt, indem die in Workshops erprobte Methodik in Software-Applikationen überführt worden ist. Zweifellos kann der Einsatz moderner Technologien die Identifikation von Risiken und ihre nachfolgenden Interpretation und Verwertung stark verbessern. Hier besteht offensichtlich noch erhebliches Potenzial sowohl in der Entwicklung, d.h. in der Schaffung massgeschneiderter Software, als auch in der Implementation bei Unternehmen und öffentlichen Institutionen. Selbstverständlich müssen entsprechende Angebote äusserst einfach zu bedienen sein, keine umfassenden Kenntnisse der dahinter stehenden Methodik oder theoretischen Grundlagen voraussetzen und natürlich zur Identifikation und Analyse von Risiken offensichtlichen Nutzen stiften. Letztlich können aber auch einfache Techniken wertvolle Dienste leisten. Im Anhang zu diesem Factsheet werden in Kurzfrom vier Methoden vorgestellt: das Brainstorming, die Delphi-Befragung, die STEEP-Analyse, und die SWOT-Analyse.

3. RISIKOIDENTIFIKATION IN DER PRAXIS

Viele Unternehmen und immer mehr Regierungen haben die zentrale Bedeutung der Risikoidentifikation erkannt. Sie haben deshalb entsprechende Systeme, Programme und Projekte lanciert, entwickelt und umgesetzt. Ihr gemeinsames Ziel besteht primär darin, anbahnende Gefahren in einer von hoher Ungewissheit geprägten Umgebung frühzeitig abzuwenden. Das gleichzeitige Nutzen von sich bietenden Zukunftschancen steht häufig noch etwas im Hintergrund, weil Risikomanagement immer noch überwiegend als die Abwehr von Ereignissen verstanden wird, die das Erreichen von definierten Zielen oder das Durchsetzen von bestimmten Wertvorstellungen verhindern könnten. Noch zu wenig wird Risikomanagement als Chancenmanagement verstanden, das mittels Erkennen von Trends und Zukunftsentwicklungen neue strategische Perspektiven und Handlungsoptionen eröffnet.

Zur Illustration von ersten Ansätzen zur Risikoidentifikation in der Praxis werden die von Versicherungen im Bereich des «Emerging Risks Management» sowie die von Regierungen unter dem Begriff des «Horizon Scanning» bekannt gewordenen Aktivitäten nachfolgend kurz dargestellt.

3.1 Emerging Risks Management in der Versicherungswirtschaft

In der Versicherungswirtschaft hat das so genannte «Emerging Risk Management» in den letzten Jahren stark an Bedeutung gewonnen. Versicherungsmanager haben in verschiedenen Umfragen solche «neuen Risiken» als bedeutend eingeschätzt und viele sehen in den (noch) unbekannten Trends und Entwicklungen – den «Unknowns» – das grösste Risiko für den Marktwert ihrer Unternehmen.[23] Dieses Interesse reflektiert sich auch in einer wachsenden Zahl von Konferenzen, Forschungsprojekten oder Industrieinitiativen wie dem Chief Risk Officer Forum und der dort angesiedelten Emerging Risk Initiative.[24] Das im ersten Kapitel genannte Beispiel des Asbests ist ein Risiko – oder eben ein Emerging Risk des beginnenden 20. Jahrhunderts (siehe Kapitel 2.1) –, das die Versicherungen während Jahrzehnten unterschätzt hatten. Die Dynamik und Unberechenbarkeit vieler dieser Risiken bedeutet, dass sie ein erhebliches Potenzial der Schadensakkumulierung aufweisen und oft mehrere Geschäftsfelder von Versicherern gleichzeitig betreffen (z. Bsp. Lebens- und Haftpflichtversicherung).

Beim Asbest beispielsweise haben die Versicherer das hohe Schadenspotenzial lange nicht erkannt bzw. verdrängt und als sie erkannt wurden, waren die auf lange Fristen angelegten Policen bereits gezeichnet. Eine weitere Herausforderung besteht darin, dass zu unbekannten Risiken oft keine Schadensstatistiken vorliegen und deshalb die traditionellen Methoden zur Festlegung von Prämien versagen.[25] Neue Risiken sind vielfach auch durch andere Policen bereits abgedeckt – natürlich unbeabsichtigterweise, da sie als solche ja nicht bekannt waren: der Versicherer sieht sich dann plötzlich mit unerwarteten Schadensforderungen konfrontiert für Fälle, die ausserhalb der Annahmen beruhen, auf deren Basis die Policen ursprünglich gezeichnet wurden – der «Fat Tail» einer vermeintlich wohl kalkulierten, «normalverteilten» Schadensstatistik gewissermassen. Weiter können gerade Risiken mit globaler Ausstrahlung – ein gutes Beispiel ist etwa eine Pandemie – enorme Konsequen-

23 Käslin, Bruno, «Early Detection and Management of Emerging Risks in the Financial Services Industry: Lessons from Insurance Businesses in Germany and Switzerland», in: Beat Habegger, *International Handbook on Risk Analysis and Management* (Zurich: Center for Security Studies, ETH Zurich, 2008), S. 155-174, hier S. 156.

24 Vgl. dazu *Chief Risk Officer Forum*.

25 Vgl. dazu und zum Folgenden Käslin, *Early Detection*, S. 159-160.

zen haben, weil viele Länder, Branchen, Personen und Geschäftsbereiche durch dasselbe Risiko gleichzeitig betroffen sind und damit die Diversifikation von Risiken als fundamentales Prinzip der Versicherungswirtschaft nicht mehr funktioniert. Schliesslich sind die Unsicherheitsfaktoren teilweise so gross und die Ursache-Wirkungsketten derart komplex, dass selbst wenn die Versicherer auf die neuen Risiken aufmerksam werden, Eintrittswahrscheinlichkeiten und konkreten Folgen sich nur schwierig abschätzen lassen.

Viele Versicherungsunternehmen haben Frühwarnsysteme etabliert, um die Herausforderungen durch neu entstehende Risiken systematisch anzugehen. Bruno Käslin hat in seiner Dissertation[26] und einem Artikel in einem vom Center for Security Studies herausgegebenen Handbuch untersucht, wie vier Versicherungsunternehmen – je zwei Erst- und zwei Rückversicherer – mit Emerging Risks umgehen. Einige für die Risikoidentifikation bedeutsame Aspekte werden nachfolgend herausgegriffen.[27]

Zunächst lässt sich sagen, dass die Unternehmen einen strukturierten und koordinierten Ansatz der Frühwarnung verfolgen. Zwar ist der Prozess nicht überall ähnlich ausgeprägt formalisiert, doch insgesamt schält sich ein Trend zu Netzwerk-basierten Früherkennungssystemen heraus: Die Unternehmen nutzen ihre externen und vor allem auch ihre internen Netzwerke – insbesondere die Mitarbeitenden – um möglichst viele und hochwertige Informationen zu sammeln. Dasselbe gilt für die Kunden, für die besondere Feedback-Kanäle geschaffen werden, sowie die Kooperation innerhalb von Branchenorganisationen. Ausserdem wird die Zusammenarbeit mit externen Experten gesucht und entsprechendes Fachwissen teilweise gezielt eingekauft. Eine koordinierende Stelle vermittelt diesen Prozess, wobei diese Projektteams bewusst heterogen zusammengesetzt sind bezüglich kulturellem Hintergrund und disziplinärer Expertise.

Das Sammeln der Informationen führt in der Regel zu einer Liste von möglichst vielen Risiken, die laufend aktualisiert und durch neu eintreffende Informationen ergänzt wird. Die Risiken werden bewertet und weiter bearbeitet, um die Informationen in verdichteter Form aufzubereiten. Dazu formulieren die Unternehmen kurze Analysen (position papers), die sich häufig in drei Teile gliedern: den wissenschaftlichen Hintergrundinformationen, einer Einschätzung des Risikos aus Sicht der Firma und der Versicherungswirtschaft insgesamt, sowie Empfehlungen zum künftigen Umgang. Diese Analysen sind natürlich laufend zu revidieren. Erstaunlicherweise werden technologie-basierte Instrumente noch wenig eingesetzt, um etwa das Internet systematisch auszuwerten oder die gesammelten Informationen zu visualisieren. Schliesslich sind die Risiken aufgrund einer Vielzahl möglicher Kriterien zu bewerten, um die Erkenntnisse gezielt in die Geschäftsstrategien einzubringen und operative Massnahmen zum Umgang mit den neu entdeckten Risiken auszulösen.

3.2 Horizon Scanning von Regierungen

Für Unternehmen der Versicherungswirtschaft ist der professionelle Umgang mit Risiken zentral für die langfristige Erhaltung ihrer Wettbewerbsfähigkeit. Interessanterweise haben auch Staaten ursprünglich in die Risikoidentifikation mit dem Ziel investiert, Entwicklungen in Forschung und Entwicklung rechtzeitig zu erkennen und so die gesamtwirtschaftliche Innovations- und damit Wettbewerbskraft zu fördern. Aus dieser Motivation heraus entwickelte sich etwa das Foresight-Programm Grossbritanniens.

26 Käslin, Bruno, *Systematische Früherkennung von Emerging Risks in der Versicherungswirtschaft* (Dissertation Universität St. Gallen, 2008).

27 Siehe zum Folgenden Käslin, *Early Detection*, S. 162-171.

Neben der Schaffung produktiver wirtschaftlicher Rahmenbedingungen ist der Schutz der nationalen Sicherheit der zweite Hauptauftrag von Regierungen. Deshalb wird nun auch in diesem Bereich vermehrt systematisch nach künftigen sicherheitspolitisch relevanten Gefährdungen gesucht. Dieser Fokus erstaunt nicht: Schliesslich besteht die Kernidee des Risikomanagements darin, Entscheidungsgrundlagen für das Handeln unter Bedingungen der Ungewissheit zu schaffen – eine Fähigkeit, die gerade in der Sicherheitspolitik essenziell ist.

Die Risikoidentifikation ist auch bei Staaten der erste Schritt eines integrierten Risikomanagements. Diese erste Phase wird häufig als Horizon Scanning bezeichnet. Es handelt sich dabei um einen strukturierten Prozess, der aktiv, kontinuierlich und systematisch nach Trends, Entwicklungen oder Ereignissen sucht, die für ein Land relevant sein könnten. Ein gutes Beispiel für diesen Scanning-Prozess bietet der so genannte «Sigma Scan» des britischen Horizon Scanning Centre (HSC).[28] Die Schaffung des HSC war Teil einer strategischen Neuausrichtung der in Grossbritannien seit langem etablierten Trend- und Zukunftsforschung. Eingeführt zur Früherkennung von Technologietrends in den sechziger Jahren, wurde diese seit Anfang des 21. Jahrhunderts zunehmend auf gesellschaftliche, ökologische und weitere Aspekte ausgeweitet.

Der Sigma Scan ist eine zentrale Aktivität des HSC und schafft eine sektorenübergreifende Informationsgrundlage für alle Regierungsaktivitäten im Bereich der strategischen Trend- und Zukunftsforschung. Für den im Dezember 2006 erstmals publizierten Scan[29] wurden bis heute Informationen aus über 2000 Quellen aus Wissenschaft, Wirtschaft, Think Tanks, Regierungen, NGOs, Blogs, Medien, Kultur, etc. ausgewertet sowie Interviews mit mehr als 300 Analysten und Experten geführt. Die Ergebnisse sind in über 270 so genannten «Issue Papers» aufbereitet, die über das Internet öffentlich zugänglich sind.[30] Alle sind bestimmten Kategorien zugeteilt und identisch aufgebaut, indem sie Hinweise geben auf bestimmte Charakteristika des Trends – beispielsweise bezüglich seiner erwarteten Entwicklung und den möglichen Auswirkungen – oder auf die Art des Trends, d.h. ob es sich um ein schwaches Signal, eine Prognose oder ein Szenario handelt. Das Ziel besteht letztlich darin, mögliche Zukunftstrends der nächsten 50 Jahre zu identifizieren und die potenziellen Auswirkungen auf die Politik Grossbritanniens abzuschätzen.[31]

Ein zweites Beispiel für ein umfassendes und zentral koordiniertes Scanning liefert Singapur. Dort wurden nach einer Reihe das Land aufrüttelnden Überraschungen – an erster Stelle ist die SARS-Epidemie von 2003 zu nennen – eine neue Sicherheitsstrategie erarbeitet, die einen vernetzten und koordinierter Ansatz zur Bewältigung der künftigen sicherheitspolitischen Herausforderungen vorsah. Als eine zentrale Massnahme wurde eine neue Einheit zur Risikofrüherkennung und -bewertung geschaffen. Dieses «Risk Assessment and Horizon Scanning»-System (RAHS) ist direkt dem Büro des Premierministers zugeordnet. Es soll die verwaltungsinterne Zusammenarbeit

28 Siehe dazu auch Habegger, Beat, *Horizon Scanning in Government: Concept, Country Experiences, and Models for Switzerland* (Zurich: Center for Security Studies, ETH Zurich, 2009).

29 Der Sigma Scan existiert seit November 2008 als fusionierter Scan aus den beiden vormals separaten Sigma Scan und Delta Scan. Der Delta Scan fokussierte auf Zukunftstrends in Wissenschaft und Forschung und stützte sich auf direkte Beiträge von führenden Experten ab. Allerdings wurde die Trennung zwischen Delta und Sigma Scan zunehmend als irreführend angesehen, weshalb ersterer nun in den Delta Scan integriert wurde.

30 *Sigma Scan*.

31 *Strategic Foresight: Antizipation und Handlungsähigkeit*, *CSS Analysen zur Sicherheitspolitik*, Nr. 52, 2009.

fördern, bessere Analyseergebnisse erzielen und exogene Schocks so früh wie möglich erkennen.

Herzstück ist ein internet-basiertes Informationssystem, an das über 20 Regierungsstellen angeschlossen sind. Dieses bündelt alle potenziell relevanten Daten und Informationen, stellt diese in der Form von Web-Services bereit und unterstützt die Nutzer mittels innovativer Anwendungen bei der Informationssuche sowie der Datenanalyse und ihrer Visualisierung. Es handelt sich um ein interoperables System, in das die Informationen dezentral eingegeben werden. Die periodische Aktualisierung der Daten erfolgt somit durch die verschiedenen angeschlossenen Behörden selber und die Informationen gelangen unvermittelt zu allen Nutzern, ohne dass eine eigentliche Koordination durch eine zentrale Stelle notwendig ist. Nun plant Singapur das RAHS weiter auszubauen, indem bestimmte Teile von RAHS mit dem Strategic Policy Office, das ebenfalls beim Premierministers angesiedelt ist und sich mit Szenarioplanung befasst, zusammenzuführen und daraus ein «Centre for Strategic Futures» zu schaffen.

3.3 Erfolgsfaktoren

Die umfassende Risikoidentifikation wie sie exemplarisch anhand der Versicherungswirtschaft und dem Horizon Scanning zweier Staaten dargestellt wurde, ist ein relativ neues Phänomen. Es wurde in der Praxis noch nicht über längere Zeit getestet und vielfach ist deshalb noch unklar, welche Ansätze, Systeme oder Programme wirklich erfolgreich sind und welche Faktoren und Kriterien in diesem Zusammenhang besonders zu beachten sind. Interessanterweise geben aber bereits die genannten und kurz dargestellten Fälle einige übereinstimmende Hinweise.[32]

Grundsätzlich lässt sich sagen, dass meistens «weiche Faktoren» wie die Kultur innerhalb der Organisation oder das Verhalten und die Einstellungen von Mitarbeitenden und Management über Erfolg oder Misserfolg entscheiden (und nicht «harte Faktoren» wie Prozesse oder Strukturen). Eine offene Risikokultur im Sinne des bewussten und proaktiven Umgangs mit Chancen und Gefahren ist in der Risikoidentifikation der zentrale Erfolgsfaktor. Konkret bedeutet dies, dass bestimmte Entwicklungen, Trends oder Ideen nicht absichtlich ausgeblendet, unangenehme Themen und Herausforderungen unterdrückt oder gar heruntergespielt werden. Vielmehr bedarf es einer offenen, von Vertrauen geprägten Kultur, in der alle Hypothesen, Vermutungen, Prognosen oder Gedankenspielereien vorgebracht werden können. Nur so entfaltet sich die kreative Kraft, die für das Entdecken von noch unbekannten Risiken essenziell ist.

Neue Informationen und Erkenntnisse zu Risiken und den möglichen Ursachen, Treibern, Wirkungen, Wahrscheinlichkeiten, Zeithorizonten oder Einflussmöglichkeiten sollten weit verbreitet werden. Zunächst gilt dies ganz besonders innerhalb von Organisationen: zuweilen stellen beispielsweise einzelne Abteilungen ihre Partikularinteressen dem Gesamtauftrag voran, indem sie nur nach den Risiken suchen, die ihren eigenen Bereich betreffen; sie schirmen sich gegen aussen ab und behalten alle Informationen für sich. Solche institutionelle Barrieren sind abzubauen und die Anreize sind so zu setzen, dass die Bereitschaft zur Weitergabe von Informationen gestärkt wird.[33] Meistens ist auch die Verbreitung von Informationen gegen aussen, d.h. jenseits der eigenen Unternehmung oder Behörde, im längerfristigen Interesse der Organisation. Dies zeigt sich bereits daran, dass auch das Entdecken von Risiken in der Regel

32 Käslin, *Early Detection*, S. 171-4; Habegger, *Horizon Scanning*, S. 25-6.

33 *Risikomanagement in der Sicherheitspolitik*, *CSS Analysen zur Sicherheitspolitik*, Nr. 30, 2008.

den Einbezug einer Vielzahl von Experten aus unterschiedlichsten Bereichen und Branchen sowie über (Landes-)Grenzen hinweg verlangt. Dasselbe gilt umgekehrt auch für die Verbreitung von Informationen: Diese muss über viele Kanäle vermittelt werden, um Aufmerksamkeit für noch wenig beachtete Themen und Probleme zu schaffen. Das breite Streuen von Erkenntnissen mobilisiert gesellschaftliche, politische oder unternehmerische Ressourcen, die der Organisation, die das Risiko entdeckt und die Information verbreitet, selber gar nicht zur Verfügung stünden. Insofern hat das Freigeben von Informationen eine «Hebelwirkung»: Es spannt Personen und Organisationen in die Suche nach Lösungen zur Minderung von Risiken ein, ohne diese dazu zu drängen oder gar dafür zu bezahlen. Dadurch nutzen weitere Organisationen diesen produktiven Mechanismus und investieren selber in die Risikoidentifikation.

Schliesslich ist eine zentrale Voraussetzung für eine offene Risikokultur die kontinuierliche Unterstützung durch die obersten Verantwortungsträger. Sie bestimmen letztlich, ob genügend Freiraum für Kreativität und Innovation vorhanden ist und ob unkonventionelle Ideen angehört, geschätzt, honoriert und nicht als Unfug herabgesetzt werden. Ausserdem können neu erkannte Risiken etablierte politische oder unternehmerische (Erfolgs-)Strategien in Frage stellen. Statt bloss abwehrend zu reagieren, bedarf es gerade in diesen Fällen ausgeprägter Führungsstärke, um die möglichen Konsequenzen neu gewonnener Erkenntnisse umfassend abzuschätzen und zu entscheiden, ob und inwiefern darauf reagiert werden soll. Idealerweise bringen sich die Entscheidungsträger deshalb direkt in den Prozess der Risikoidentifikation ein und die Stellen, die dafür innerhalb einer Organisation verantwortlich sind, sollten möglichst nahe an die obersten Entscheidungsebenen rapportieren.

3.4 Blick auf die Schweiz

Wie alle Staaten muss auch die Schweiz ihre Gefahren kennen. Deshalb braucht sie ebenfalls einen umfassenden Prozess der Risikoidentifikation, um bedrohungsgerechte politische Massnahmen zu formulieren und umzusetzen. Die Verwaltung hat in der Vergangenheit zahlreiche Risiko- und Verwundbarkeitsanalysen initiiert, die allerdings nur wenig erfolgreich waren.[34] Der Bedarf an einer umfassenden und querschnittsorientierten Risikoanalyse, die über die sektorspezifischen Untersuchungen einzelner Behörden hinausgeht, besteht aber weiterhin. Das Bundesamt für Bevölkerungsschutz hat deshalb Anfang 2009 einen neuen Anlauf unternommen. Unter dem Titel «Risiken Schweiz» will es die für die Schweiz relevanten Bedrohungen und Risiken erfassen und bewerten. Dieses Vorgehen mündet letztlich in eine nationale Gefährdungsanalyse und fügt sich insofern in ähnliche Bemühungen anderer Staaten ein (auch wenn das Projekt derzeit natürlich noch weit von den aufwändigen Programmen Grossbritanniens oder Singapurs entfernt ist). Welche Ergebnisse sich letztlich im anspruchsvollen föderalen Umfeld der Schweiz erzielen lassen, werden die nächsten Jahre zeigen. Empfehlenswert ist aber sicherlich, bereits heute erste Optionen zu entwickeln, wie die Risikoidentifikation als Daueraufgabe etabliert werden kann und wie sich die Synergien zwischen Bund und Kantonen sowie innerhalb der Verwaltung optimal ausschöpfen lassen.

34 Siehe dazu Bonin, Sergio und Beat Habegger, «*Risiko- und Verwundbarkeitsanalyse in der Bundespolitik: Erfahrungen und Perspektiven*», in: Wenger, Andreas, Victor Mauer und Daniel Trachsler (Hrsg.), *Bulletin zur Schweizerischen Sicherheitspolitik 2009* (Zürich: Center for Security Studies ETH Zürich, 2009), S. 35-55.

4. SCHLUSSFOLGERUNGEN

Risikomanagement hat sich in der Vergangenheit stark an quantifizierbaren Daten und mathematischen Modellen orientiert und diese in eine komplexe Architektur von Strukturen und Prozessen eingebettet. Darob ging zuweilen vergessen, dass Quantität die mangelnde zugrunde liegende Qualität von Informationen nicht auszugleichen vermag.[35] Ausserdem ist zu viel Komplexität einem effizienten und wirkungsorientierten Umgang mit Risiken eher abträglich. Die Ursachen und der Verlauf der gegenwärtigen Finanz- und Wirtschaftskreise liefern dafür beste Beispiele. Strategische Überraschungen sind auch in Zukunft zu erwarten und verlangen nach einer kreativ vorausschauenden Risikoidentifikation.

Oberstes Ziel von Risikomanagement ist es, Risiken präventiv zu verhindern und für den Fall, dass sie sich doch ereignen, die nötigen Vorkehrungen zu treffen, um den Schaden möglichst gering zu halten. Die rechtzeitige Identifikation von Risiken und ihre kontinuierliche Überwachung ist die erste grundlegende Phase eines integrierten Risikomanagements. Es geht somit primär darum, ein wirklich umfassendes Bild der Risikolandschaft in all ihren Dimensionen zu erlangen. Dafür ist, erstens, zu verhindern, dass Organisationen eine zu ausgeprägte «Innensicht» einnehmen und nur ungenügend über die eigenen Grenzen und den eigenen Wirkungs- und Interessenbereichs hinausschauen. Wer will, sieht immer nur die Risiken, die einen selber bzw. den eigenen Tätigkeitsbereich betreffen; alles andere lässt sich einfach ausblenden oder gar für nicht relevant erklären. Zweitens gilt es nicht ausschliesslich auf Einzelrisiken zu fokussieren, sondern besonders die Interdependenzen, Verbindungen und Schnittstellen zwischen Risiken zu beachten. Deshalb braucht es, drittens, Analysten und Entscheidungsträger, die Expertise mit kreativem Denken zu verbinden wissen. Verschiedene Ausbildungen, Berufe oder kulturelle Prägungen erlauben unterschiedliche Blicke auf mögliche Risiken und erlauben einen ganzheitlicheren und umfassenderen Bild auf eine komplexe Risikolandschaft.

35 *Re-Thinking Risk Management: Why the Mindset Matters More Than the Model*, *Knowledge@Wharton*, 15 April 2009.

AUSGEWÄHLTE ERGÄNZENDE LITERATUR

Bracken, Paul, Ian Bremmer and David Gordon (eds.), *Managing Strategic Surprise: Lessons from Risk Management and Risk Assessment* (Cambridge: Cambridge University Press, 2008).

Bremmer, Ian and Preston Keat, *The Fat Tail: The Power of Political Knowledge for Strategic Investing* (Oxford: Oxford University Press, 2009).

Chun Wei Choo, *Information Management for the Intelligent Organization: The Art of Scanning the Environment* (Medford: Information Today, 2002).

European Environmental Agency, *Late lessons from Early Warnings: The Precautionary Principle 1896–2000* (Environmental Issue Report No. 22, Copenhagen, 2001).

Fink, Alexander und Andreas Siebe, *Handbuch Zukunftsmanagement: Werkzeuge der strategischen Planung und Früherkennung* (Frankfurt: Campus, 2006).

Habegger, Beat, *Handbook on Risk Analysis and Management: Professional Practices* (Zurich: Center for Security Studies, ETH Zurich, 2008).

Käslin, Bruno, *Systematische Früherkennung von Emerging Risks in der Versicherungswirtschaft* (Dissertation Universität St. Gallen, 2008).

Krystek, Ulrich und Günter Müller-Stewens. *Frühaufklärung für Unternehmen: Identifikation und Handhabung zukünftiger Chancen und Bedrohungen* (Stuttgart: Schäffer-Pöschel, 1993).

Taleb, Nassim Nicholas, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007)

ANHANG: INSTRUMENTE UND METHODEN FÜR DIE PRAXIS

STEEP-Analyse

In Kürze	Die STEEP-Analyse ist ein Instrument zur systematischen Analyse aller relevanten Umwelten einer Organisation und ihrer Strukturierung in vorgängig definierte Kategorien. Bei diesen Kategorien handelt es sich um soziale (social), technologische (technological), wirtschaftliche (economic), ökologische (environmental) und politische (political) Faktoren (STEEP). Je nach untersuchter Organisation bzw. dem relevantem Umfeld können weitere Kategorien hinzukommen, etwa rechtliche (legal), ethische (ethical) oder demographische (demographical) Faktoren. Dies erklärt, weshalb diese Analysen auch STEEP, PESTE, PESTLE, SLEPT, STEEPLED, etc. genannt werden.
Ziel und Zweck	Eine STEEP-Analyse hat zum Ziel, alle relevanten Umweltfaktoren, die auf eine Organisation wirken können, auf übersichtliche Weise zu kategorisieren. In ihrer einfachsten Form, leistet sie eine simple Auflistung von Faktoren in definierten Kategorien. Darüber hinaus können die derart strukturierten Informationen entweder in Kombination mit anderen Methoden weiter bearbeitet werden, oder als «Rohmaterial» in zusätzliche Analysen – etwa die SWOT-Analyse – einfliessen.
Wichtigste Schritte	1. *Definition des zu analysierenden Systems* (z. Bsp. eine bestimmte Organisation). 2. *Festlegung* der relevanten analytischen Kategorien. 3. Diese Kategorien (z. Bsp. STEEP) werden genutzt, um systematisch alle relevanten Faktoren im Umfeld einer Organisation zu *identifizieren*. Dazu lassen sich viele Methoden einsetzen wie etwa Umfragen, Interviews, Brainstormings, etc. ◆ *Weiterverarbeitung* der gesammelten und strukturierten Informationen
Bewertung	Stärken: ◆ Einfach durchzuführen ◆ Viele unterschiedliche Faktoren lassen sich systematisch identifizieren und auf leicht verständliche Weise strukturieren Schwächen: ◆ In ihrer «Rohform», hat die STEEP-Analyse wenig analytischen Gehalt ◆ Zur Analyse der identifizierten Faktoren hinsichtlich Ursachen, Wirkungen, Interaktionen und Dynamik braucht es weiterführende Methoden
Anwendungen	STEEP-Analysen wurden ursprünglich im strategischen Management und Marketing genutzt. Allerdings lässt sich diese zur Analyse des externen Umfelds von eigentlich allen Systemen und Organisationen verwenden werden. Sie wird deshalb auch in der Politikanalyse oder im Risikomanagement oft eingesetzt.
Quellen	Eurescom, *STEEP Analysis for the year 2010: United Kingdom, Norway, and Hungary* (2007) World Economic Forum, *Global Risks 2007: A Global Risk Network Report* (Cologny/Geneva: World Economic Forum, 2007), S. 6.

Brainstorming

In Kürze	Brainstorming umfasst eine Vielzahl von Methoden zur Förderung der Kreativität und zur Entwicklung neuer Ideen. Zwei Prinzipien sind zentral: Erstens sind während des Brainstormingprozesses die Ideen weder zu bewerten noch zu beurteilen; Kritik ist unerwünscht. Zweitens gilt die Vermutung, dass mehr Ideen immer besser sind, da es wahrscheinlicher wird, dass sich eine wertvolle darunter befindet. Selbst wenn eine Idee nicht direkt zur Problemlösung beiträgt, stimuliert sie doch den kreativen Prozess und inspiriert zur Entwicklung weiterer Ideen.
Ziel und Zweck	Brainstorming gibt es vielen Varianten. Einige Beispiele: ◆ *Klassisches Brainstorming in der Gruppe*: Das Problem ist dabei, dass oft einzelne Personen dominieren sowie Mitläufereffekte und «Groupthink» entstehen können. ◆ *Brainwriting*: Alle schreiben ihre Ideen auf. Anschliessend werden sie entweder durch die Teilnehmenden mündlich vorgestellt oder sie werden schriftlich verteilt und als neuer Input für weiteres individuelles Brainwriting verwendet. ◆ *6-3-5*: 6 Leute notieren auf je einer Karte 3 Ideen; sie geben die Karten (5-mal) weiter und ergänzen die erhaltenen Karten jeweils wieder mit ihren eigenen Ideen. Das Ziel ist stets, dass sich die Teilnehmenden fortlaufend kreativ anregen und durch ihren gegenseitigen Austausch immer neue Ideen hervorbringen.
Wichtigste Schritte	1. *Angenehme Umgebung schaffen*: Eine entspannte Atmosphäre ohne Ablenkungen oder gar Störungen erlaubt die notwendige Konzentration. 2. *Anzahl Teilnehmende*: Idealerweise zwischen sechs und zwölf Personen, die bevorzugt verschiedene Erfahrungen, Prägungen, Herkünfte, etc. einbringen. 3. *Problemdefinition*: Die Themenstellung ist durch den Moderator so neutral und objektiv wie möglich – nicht zu eng und nicht zu ausschweifend – zu definieren. 4. *Moderation*: Strukturiert den Ablauf, sorgt für die Einhaltung der Regeln, beachtet die Gruppendynamik und interveniert falls nötig, ermutigt zur Ideenentwicklung und nimmt keinerlei Wertungen vor. 5. *Aufzeichnung*: Alle Ideen werden aufgezeichnet und kommuniziert.
Bewertung	Stärken: ◆ Fördert kreative Prozesse: Verbessert die Fähigkeit zur Entwicklung neuer Ideen und Lösungswege sowie zur Antizipation von Problemen ◆ Stark in relativ unstrukturierten Situationen mit vielen unbekannten Einflussfaktoren Schwächen: ◆ Stark subjektiver Prozess: anfällig für kognitive Verzerrungen und Fehleinschätzungen ◆ Gruppendynamik ist schwierig zu kontrollieren und kann Ergebnisse verzerren ◆ Wenig hilfreich bei klar definierten Problemen und in Entscheidsituationen
Anwendungen	Brainstorming ist vermutlich die bekannteste und am weitesten verbreitete Kreativitätstechnik. Sie wurde entwickelt von Alex Osborn in den 1940er Jahren zur Problemlösung in seiner Werbeagentur und hat sich rasch in alle Bereiche von Wirtschaft und Gesellschaft ausgebreitet.
Quellen	Clark, Charles, *Brainstorming: How to Create Successful Ideas* (Chatsworth, CA: Wilshire Book Company, 1989). Gilhooly, K. J., *Thinking: Directed, Undirected and Creative* (London: Academic Press, 2nd ed., 1990). Osborn, Alex F., *Applied Imagination* (New York: Charles Scribner and Sons, 1953). Rickards, Tudor, *Creativity and Problem Solving at Work* (Aldershot: Gower, 1990).

Delphi-Befragung

In Kürze	Eine Delphi-Befragung – der Begriff leitet sich vom Orakel der Antike ab – ermittelt Einschätzungen oder Prognosen von Experten zu Trends, Entwicklungen oder Ereignissen der Zukunft. Unabhängige Experten werden in mehreren Interviewrunden zu einem bestimmten Thema oder Problem befragt und nach jeder Runde mit den (anonymisierten) Antworten der anderen Teilnehmenden konfrontiert. Sobald sich die ermittelten Antworten der Teilnehmer nicht mehr wesentlich ändern, wird die Befragung beendet und die Ergebnisse bzw. Prognosen der letzten Runde werden in einem Schlussbericht zusammengeführt.
Ziel und Zweck	Ziel einer Delphi-Befragung ist es, einen Expertenkonsens zu ermitteln. Dieser soll sich durch mehrere Interviewrunden und vor allem die Rückkoppelungsprozesse, bei denen die Experten jeweils mit den Antworten ihrer «Peers» konfrontiert werden, herausbilden. Dadurch sollen sich die Antworten schrittweise annähern und weniger «subjektiv» werden, bis sich letztlich ein Konsens herausbildet.
Wichtigste Schritte	◆ *Identifikation von Experten*: Zentrales Kriterium ist relevantes Fachwissen. ◆ *Testen des Fragebogens und Einladung an Experten*: Je nach Untersuchung sind 10 bis 50 Experten ideal. Die Teilnahmebereitschaft steigt, wenn die Experten wissen, durch wen sie vorgeschlagen wurden. ◆ *Erste Interviewrunde*: Alle Experten erhalten den Fragebogen; ihre Antworten werden dann in einem Dokument zusammengefasst und nur minimal bearbeitet. ◆ *Zweite Interviewrunde*: Mit dem zweiten Frageboden erhalten die Experten eine anonymisierte Fassung der Antworten aller Experten aus der ersten Interviewrunde; die neuen Fragen können sich spezifisch auf Antworten der ersten Runde beziehen und so nach Präzisierungen oder genaueren Ausführungen fragen. ◆ *Weitere Interviewrunden*: Dieser iterative Prozess von Befragung und Rückkoppelung kann über mehrere Runden hinweg weitergeführt werden. ◆ *Schlussbericht*: Sobald sich ein Konsens herausgebildet hat, werden die Ergebnisse in einem Bericht zusammengefasst und an alle Teilnehmenden verschickt.
Bewertung	Stärken: ◆ Neuestes Expertenwissen wird systematisch ermittelt ◆ Anonymität fördert die freie Meinungsäusserung und Kritik; sie mindert zugleich die Verzerrungen offener Gruppeninteraktionen ◆ Befragungen sind an keinen Ort und keine bestimmte Zeit gebunden Schwächen: ◆ Tendenz zur Befragung etablierter Experten; Aussenseiter und Querdenker werden oft nicht eingeladen ◆ Fraglich, ob sich Zukunftstrends aus einem Expertenkonsens ableiten lassen: Extrempositionen und Minderheitsmeinungen werden eliminiert ◆ Relativ zeit- und arbeitsintensiv
Anwendungen	Die Delphi-Befragung wurde in den 1950er Jahren durch die RAND Corporation entwickelt mit dem Ziel, einen Konsens unter amerikanischen Militärexperten zu ermitteln. Später wurde die Methode in Forschung und Entwicklung intensiv genutzt und bald auch zur Ermittlung von Trends in Wirtschaft und Gesellschaft eingesetzt. Die Zuverlässigkeit der Resultate von Delphi-Befragungen und ihr Leistungsausweis insgesamt sind wissenschaftlich umstritten. Deshalb wird sie heute weniger genutzt.
Quellen	Häder, Michael and Sabine Häder (eds.), *Die Delphi-Technik in den Sozialwissenschaften* (Wiesbaden: Westdeutscher Verlag, 2000). Linstone, Harold A. and Murray Turoff (eds.), *The Delphi Method: Techniques and Applications* (Reading: Addison-Wesley, 1975)

SWOT-Analyse

In Kürze

Mit einer SWOT-Analyse lassen sich Informationen zur internen Lage und den äusseren Einflussfaktoren einer Organisation strukturiert darstellen. Sie bietet einen «interpretativen Filter», mit dem sich grosse Informationsmengen in einfache Kategorien gliedern und daraus strategische Entscheidungsalternativen ableiten lassen. SWOT steht für Stärken (strengths), Schwächen (weaknesses), Chancen (opportunities) und Gefahren (threats).

Ziel und Zweck

Eine SWOT-Analyse hat zwei zentrale Ziele:

- Sie hilft, die wichtigsten internen und externen Faktoren, die auf eine Organisation wirken, strukturiert zu sammeln und darzustellen.
- Mittels der identifizierten Schlüsselfaktoren können strategische Handlungsalternativen identifiziert und entwickelt werden.

Wichtigste Schritte

1. *Sammlung umfassender Informationen* zu allen Dimensionen (SWOT), möglicherweise in Kombination mit anderen methodischen Ansätzen.
2. *Interne Analyse*: Identifizieren der Stärken und Schwächen der Organisation, die sie typischerweise selber beeinflussen kann.
3. *Externe Analyse*: Chancen und Gefahren (Einflussfaktoren und Treiber) im Umfeld der Organisation, die sie betreffen, ohne sie selber direkt beeinflussen zu können.
4. *Ausarbeitung strategischer Alternativen*: Stärken und Chancen bilden Ansatzpunkte zum Erreichen von Zielen; Schwächen und Gefahren weisen auf zu beseitigende Hürden hin. Die folgenden grundlegenden Handlungsstrategien sind möglich:

	Chancen	Gefahren
Stärken	A	B
Schwächen	C	D

Feld A: die Organisation nutzt ihre Stärken, um Chancen in ihrem Umfeld wahrzunehmen; *Feld B*: sie nutzt ihre Stärken, um künftige Gefahren abzuwenden; *Feld C*: externe Chancen helfen interne Schwächen zu überwinden; *Feld D*: eigene Schwächen sind zu reduzieren, um die Verwundbarkeit gegenüber externen Gefahren abzubauen.

Bewertung

Stärken:

- Einfach zu konstruieren und intuitiv verständlich
- Unterscheidung in interne und externe Faktoren ergibt ein strukturiertes Informationsprofil
- Einfaches Ableiten erster grober strategischer Handlungsoptionen

Schwächen:

- Simplifizierend und reduktionistisch
- Interdependenzen zwischen den Faktoren werden ausgeblendet
- Meistens werden zu viele Faktoren aufgelistet ohne Gewichtung und Priorisierung

Anwendungen

SWOT-Analysen wurden ursprünglich vor allem in den Bereichen Marketing und strategisches Management eingesetzt. Es ist vermutlich eine der am meisten verwendeten Methoden der Unternehmensanalyse und Strategieentwicklung. Mittlerweile ist sie auch in der Plannung und Politikentwicklung öffentlicher Institutionen fest verankert.

Quellen

Bryson, John M. und William D. Roering, «Applying Private-Sector Strategic Planning in the Public Sector», *Journal of the American Planning Association*, 53(1), 1987, 9-22.

European Commission, *The GUIDE: Evaluating Socio-Economic Development; Policies, Programmes, Themes and Projects*.

Müller-Stewens, Günter, «Strategische Entwicklungsprozesse», in: Rolf Dubs et al. (Hrsg.), *Einführung in die Managementlehre*, vol. 2 (Bern: Haupt, 2004), S. 39–83.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** specializes in research, teaching, and information services in the fields of international relations and security policy. The CSS also acts as a consultant to various political bodies and the general public. The Center is engaged in research projects with a number of Swiss and international partners, focusing on new risks, European and transatlantic security, strategy and doctrine, state failure and state building, and Swiss foreign and security policy.

The **Crisis and Risk Network (CRN)** is an Internet and workshop initiative for international dialog on national-level security risks and vulnerabilities, critical infrastructure protection (CIP) and emergency preparedness.

As a complementary service to the International Relations and Security Network (ISN), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland. (www.crn.ethz.ch)