Blackout

Eine nationale Herausforderung bereits vor der Krise

Herbert Saurugg
Wien, Jänner 2012

Vorwort

Die Forschungs- und Seminararbeit *„Blackout - Eine nationale Herausforderung bereits vor der Krise“* wurde im Rahmen des Masterstudiengangs „Unternehmensentwicklung" an der Hochschule für Management Budapest (AVF), mit dem inhaltlichen Schwerpunkt "Kritische Infrastrukturen", erstellt.

Aufgrund der hohen Aktualität wird sie unter der Creative Commons Lizenz (by-nc-sa)[1] zur allgemeinen Sensibilisierung und als Basismaterial für weitere Bearbeitungen öffentlich zur Verfügung gestellt.

Hintergrund zum Autor

Seit 15 Jahren Berufsoffizier beim österreichischen Bundesheer; Akademischer Sicherheitsexperte für Informations- und Kommunikationstechnik; Ausgebildeter Projektmanager (PMA); Ausgebildeter Krisen- und Notfallmanager, BdSI.

Bildquelle Titelfoto: http://www.energieverbraucher.de

1 URL: https://secure.wikimedia.org/wikipedia/de/wiki/Creative_Commons [10.01.2012]; by: Namensnennung, nc: nicht kommerziell, sa: Weitergabe unter gleichen Bedingungen.

Inhaltsverzeichnis

Sprachliche Gleichbehandlung:

In weiterer Folge beziehen sich, um die Lesbarkeit zu erleichtern, so weit auf natürliche Personen bezogene Bezeichnungen nur in männlicher Form angeführt sind, diese auf Frauen und Männer in gleicher Weise.

Executive Summary

Fast unsere gesamte lebens- und überlebensnotwendige Infrastruktur hängt von der Verfügbarkeit der Stromversorgung ab. Ein Ausfall der bisher sehr zuverlässigen Stromversorgung würde innerhalb kürzester Zeit verheerende Folgen nach sich ziehen.

Aufgrund der im Rahmen der Analyse der geplanten Einführung von intelligenten Stromzählern gewonnenen Erkenntnisse[1] und der aktuellen Berichterstattung, erfolgte eine vertiefende Betrachtung des Themas „Blackout". Unter Blackout ist in dieser Arbeit ein plötzlicher, großräumiger, länger andauernder Stromausfall zu verstehen. Ziel war die Verifizierung, ob es sich hier um einen Hype[2], oder um eine reale Bedrohung handelt.

Seit wenigen Jahren gibt es zahlreiche schwerwiegende Eingriffe in das komplexe System der europäischen Stromversorgung, wie nun auch eine Analyse der deutschen Bundesnetzagentur, die Anfang 2012 veröffentlicht wurde, festhält:

> *„Der hierfür notwendige Umbau des Versorgungssystems erfolgt dabei am 'offenen Herzen', nämlich im Vollbetrieb und aus Netzperspektive zunehmend an seiner Grenze."*[3]

Die Auswirkungen auf die zukünftige Stromversorgungssicherheit sind daher nicht wirklich absehbar. Wie sich im Rahmen der Analyse herausgestellt hat, gibt es derzeit sehr viele Anhaltspunkte, dass es sich beim Thema Blackout um eine reale Bedrohung handelt. Ganz wesentlich dabei ist, dass es sich aufgrund des eng vernetzten, europäischen Verbundsystems um keine reine nationale Angelegenheit handelt. Es kann durchaus davon ausgegangen werden, dass die Auslösung eines möglichen Blackouts nicht in Österreich stattfindet. Darüber hinaus liegen mehrere Aussagen von österreichischen Netzbetreibern vor, dass bei einem österreichweiten Blackout die Stromversorgung unter günstigen Voraussetzungen erst nach etwa 24 Stunden wieder weitgehend hergestellt werden kann. Seriöse Kostenanalysen erwarten bei einer österreichweiten Stromversorgungsunterbrechung, abhängig von der Jahres- und Tageszeit, Schäden von bis zu 900 Millionen Euro pro Tag.

Ein weiteres Ergebnis der Analyse ist, dass der Großteil der Gesellschaft – mit einigen Ausnahmen, vom einfachen Bürger bis zur nationalen Katastrophenhilfe – über keine ausreichenden Bewältigungskompetenzen verfügt. Dies ist vor allem auf den Widerspruch zwischen Risikowahrnehmung und der Realität zurückzuführen. Es fehlt weitgehend an einem entsprechenden Risikobewusstsein, an adäquaten Krisenpräventionsmaßnahmen und insbesondere an der Selbsthilfefähigkeit der Bevölkerung. Dies ist auf die de-facto nicht vorhandene Risikokommunikation, die Vermittlung des Umgangs mit Unsicherheiten und Gefahren, zurückzuführen. Besonders nachteilig im Fall eines Blackouts ist die mangelnde Selbsthilfefähigkeit und Eigenvorsorge der Bevölkerung, welche für eine Schadensminimierung ganz wesentlich sind. Auf der organisatorischen Ebene ist die Bewältigung eines möglichen Blackouts nicht auf rein regionaler Ebene möglich und wird wahrscheinlich sogar eine länderübergreifende Koordinierung erfordern. Diese erfordert aber eine präventive Vorbereitung.

Überraschend war nach der Analyse der verschiedensten Quellen auch die Erkenntnis, dass in der Regel sehr einseitig gedacht und analysiert wird, vor allem mit Fokus auf mögliche Vorteile, selten auf eventuelle Nachteile. Diese Erkenntnis ist wahrscheinlich auf ein noch zu we-

1 Vgl. Saurugg, 2011b.

2 Übertriebene und aufgebauschte, meist kurzlebige, Nachricht.

3 Vgl. Bundesnetzagentur, 2011b, S. 47.

nig ausgeprägtes vernetztes Denken zurückzuführen. Hier sind vor allem die Bildungs- und Forschungseinrichtungen gefragt. Einerseits in der Wissensvermittlung und andererseits bei der konkreten Forschungsarbeit, diesem Manko entgegenzuwirken.

Eine zukünftig große Herausforderung wird die möglichst klare Trennung zwischen Erfordernissen des Marktes und jenen, welche für die Überlebensfähigkeit von Systemen und Infrastrukturen von entscheidender Bedeutung sind. Derzeit ist häufig eine langfristig gesehen, kontraproduktive Vermischung und damit auch Irreführung der Entscheidungsträger zu beobachten.[4] Marktwirtschaftliche Interessen spiele dabei eine große Rolle.

Die vorliegende Analyse dient keinesfalls der „Panikmache“ oder als „Weltuntergangsszenario“, sondern soll viel mehr zu einer Sensibilisierung des Lesers und vor allem der Verantwortungs- und Entscheidungsträger beitragen. Risiken zu überleben ist ein wichtiger Bestandteil der Evolution und Motor für Weiterentwicklungen. Damit dies möglich ist, muss aber auch eine aktive Auseinandersetzung mit diesen erfolgen. Hierbei gibt es grundsätzlich zwei Möglichkeiten – präventiv oder reaktiv. Reaktiv führt zur Einschränkung der Handlungsfreiheit und bedeutet in der Regel, unter in Kaufnahme von Verlusten, was heute selten akzeptiert wird. Der entscheidende Punkt dabei ist, dass die Wahrnehmung von Risiken von Emotionen abhängt und es keine Veränderung ohne Emotionen gibt.[5]

Die Conclusio dieser Arbeit ist, dass das Thema Blackout durchaus eine reale Bedrohung für unsere Gesellschaft darstellt. Gleichzeitig muss aber auch betont werden, dass wir unserer Zukunft nicht hilflos ausgeliefert sind, sondern den Verlauf selbst mitbestimmen können und müssen.

Eine weitere Vertiefung im Bereich der möglichen Krisenprävention und -reaktionsfähigkeiten ist im Rahmen der folgenden Masterarbeit beabsichtigt.

„Deshalb ist es Zeit, umgekehrt zu denken und die als zu verwirklichenden Veränderungen vom Endziel her ausgehend und nicht die Ziele von den verfügbaren Mitteln und den sofort zu stopfenden Löchern her zu definieren.“

André Gorz, Sozialphilosophe, aus „Die entzauberte Arbeit“

4 Vgl. Bundesnetzagentur, 2011b.

5 Vgl. Witzer, 2011, S. 105ff.

1 Einleitung

In der ersten Seminararbeit *„Der Cyberspace und die Auswirkungen auf die nationale Sicherheit“*[6] wurden mehrere Beispiele wie etwa Stuxnet, Conficker, SCADA Systeme, Smart Grids, Smart Meter, Social Engineering zur Darstellung des Gefährdungspotentials aus dem Cyberspace, vor allem mit möglichen Auswirkungen auf die nationale Sicherheit, analysiert.

> ***Nationale Sicherheit:*** *„Die Fähigkeit einer Nation, ihre inneren Werte vor äußerer Bedrohung zu schützen.“*[7]

Es erfolgte in kurzer Form eine Gegenüberstellung der derzeit verfügbaren nationalen Instrumente zur Krisenbewältigung. Dies führte zur Erkenntnis, dass die derzeit verfügbaren nationalen Ressourcen und Strukturen zur Bewältigung von Schadensereignissen, die durch komplexe Angriffe aus dem Cyberspace ausgelöst werden können, wahrscheinlich nicht ausreichen werden.

In der zweiten Seminararbeit *„Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit“*[8] erfolgte eine Vertiefung in die aktuelle Problematik der unkritischen Einführung und Implementierung von intelligenten Stromzählern („Smart Meter“). Wie sich bei der Bearbeitung herausstellte, gibt es hierzu erhebliche Sicherheitsbedenken. Dies insbesondere, da es kaum adäquate Risikoanalysen und -bewertungen gibt und gleichzeitig massiv in die wichtigste Infrastruktur unserer heutigen Gesellschaft – die Stromversorgung – eingegriffen wird. Die Folgen sind derzeit nicht absehbar. Als de-facto Nebenprodukt dieser Arbeit ergab sich die Betrachtung des Themas Blackout.

> **Blackout:** Hinter dem englischen Begriff verbirgt sich die etwas sperrige Beschreibung für einen plötzlichen, großräumigen und länger andauernden Stromausfall, wobei es keine klare quantitative Eingrenzung gibt.[9] In dieser Arbeit wird mit dem Begriff Blackout ein Stromausfall in einem großflächigen Gebiet, sodass nicht einfach externe Hilfe zugeführt werden kann, bzw. über eine Dauer von länger als eine Stunde assoziiert.

Aufgrund der ersten Erkenntnisse und der sehr weitreichenden Folgen eines Blackouts erfolgte die Entscheidung, dieses Thema im Rahmen der dritten Seminararbeit weiter zu vertiefen. Dabei war von Anfang an bewusst, dass durch die hohe Komplexität eine umfassende Betrachtung nicht möglich sein wird.

Die wesentlichen Forschungsfragen für diese Analyse lauten daher:

1. **Sind Blackouts eine reale Bedrohung oder reine „Angstmacherei“?**
2. **Ist das nationale Krisen- und Katastrophenschutzmanagement ausreichend auf ein solches Szenario vorbereitet?**
3. **Besteht Handlungsbedarf? Wenn ja, in welchen Bereichen?**

6 Vgl. Saurugg, 2011a.
7 Woyke, Wichard (Hrsg.): *Handwörterbuch internationale Politik.* Opladen: Barbara Budrich, 2006 , S. 288.
8 Vgl. Saurugg, 2011b.
9 Vgl. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 4.

1.1 Vorgangsweise bei der Bearbeitung

Bisher gab es in Europa kaum schwerwiegende Zwischenfälle mit großräumigen und länger andauernden Stromausfällen. Daher sind entsprechende Rückschlüsse über die Tragweite eines solchen Ereignisses kaum bzw. nur in kleinen Fachkreisen vorhanden. Immer wieder wird mit „Da bisher nichts passiert ist, wird auch in Zukunft nichts passieren." oder „Dieses Problem ist in Österreich aufgrund der sehr guten Infrastruktur derzeit nicht relevant." argumentiert. Diese Antworten lassen auf ein stark lineares Denken rückschließen. Ein Schluss, der trügerisch und auch gefährlich sein kann. Um diese Annahmen zu verifizieren, werden einige Beispiele von folgenschweren Ereignissen im Kapitel Krisen- und Katastrophenereignisse analysiert, die eigentlich nicht passieren hätten dürfen. Vorangestellt erfolgt im Kapitel Komplexe Systeme und die Stromversorgung eine kurze Einführung in die Kybernetik, welche für die weitere Betrachtung sehr wesentlich ist. Dabei wird gleich, wo möglich, ein Bezug zur Stromversorgung hergestellt.

Das Schwergewicht wird im Kapitel Stromversorgungssicherheit auf die Analyse des derzeitigen, im Umbruch befindlichen, Stromversorgungssystems gelegt. Insbesondere soll dabei festgestellt werden, ob es konkrete Hinweise auf mögliche Schwachstellen bzw. kritische Systemvariablen gibt, die ein Blackout begünstigen können. Der Fokus liegt dabei auf Faktoren, die gegenwärtig und jederzeit für ein Blackout ausschlaggebend sein könnten.

Im Kapitel Der Zivilschutz in Österreich wird der derzeitige Status des österreichischen Krisen- und Katastrophenschutzes und die Bewältigungskompetenz für ein solches Szenario analysiert.

Im Schlusskapitel Schlussfolgerungen erfolgen abschließende Betrachtungen und Denkanstöße für weitere Bearbeitungen.

1.2 Begrifflichkeiten

Einige Begriffe, wie Gefahr/Gefährdung/Risiko, oder auch Krise/Katastrophe werden in dieser Arbeit immer wieder verwendet. Da es generell, je nach Kontext, sehr unterschiedliche Definitionen gibt, erfolgt eine kurze Zusammenfassung und Beschreibung der wesentlichen Begriffe. Zum Teil werden auch bewusst mehrere Beschreibungen herangezogen, um den Fokus nicht zu sehr einzuengen, da eine klare Abgrenzung bei einem derart komplexen Thema vermutlich falsch wäre.

1.2.1 Dominoeffekt

Unter einem Dominoeffekt wird eine „Abfolge von Ereignissen, von denen jedes einzelne Ereignis zugleich Ursache für das nachfolgende ist; alle Ereignisse sind auf ein und dasselbe Anfangsereignis zurückzuführen."[10] verstanden. Der Begriff kann durchaus als Synonym für einen Kaskadeneffekt verwendet werden.

10 Bundesministerium des Innern, 2005, S. 51.

1.2.2 Gefahr

„Eine Gefahr ist eine Situation oder ein Sachverhalt, der zu einer negativen Auswirkung führen kann. Diese negative Auswirkung einer Gefährdung kann Personen, Sachen, Sachverhalte, Umwelt oder Tiere treffen.“[11]

1.2.3 Gefährdung

„Eine Gefährdung bezieht sich ganz konkret auf eine bestimmte Situation oder auf ein bestimmtes Objekt und beschreibt die Wahrscheinlichkeit mit der eine potenzielle Gefahr zeitlich oder räumlich auftritt.“[12]

1.2.4 Interdependenzen

Interdependenzen sind „Wechselseitige Abhängigkeiten bzw. Beeinflussungen von Variablen, z. B. Infrastrukturen.“[13]

„Durch Interdependenzen (Abhängigkeiten zwischen den einzelnen Sektoren oder Branchen) wird das Risiko von Ausfällen noch verstärkt. Ausfälle in einem Sektor können zu Ausfällen in anderen Sektoren führen und auf diese Weise einen Dominoeffekt auslösen. Besonders brisant sind wechselseitige Abhängigkeiten d. h. der Ausfall einer Infrastruktur führt zum Ausfall einer weiteren Infrastruktur, die ihrerseits aber wieder Voraussetzung zur störungsfreien Funktion der zuerst ausgefallenen Infrastruktur ist. Eine solche Situation besteht teilweise zwischen Informations- und Kommunikationstechnik und bestimmten Bereichen der Energieversorgung bei längerfristigen Ausfällen.“[14]

1.2.5 Katastrophe

„Als Katastrophe ist jedes bereits eingetretene oder noch bevorstehende Ereignis zu verstehen, das durch elementare, technische oder sonstige Auswirkungen geeignet ist, in ungewöhnlichem Ausmaß Personen- oder Sachschäden zu bewirken und das mit örtlichen Einsatzkräften nicht bewältigt werden kann.“[15]

oder

„Eine Ausnahmesituation, die Menschen in ihren täglichen Lebensgewohnheiten unterbricht, welche infolgedessen Schutz, Nahrung, Kleidung, Unterkunft, medizinische und soziale Fürsorge benötigen. Kann dies nicht mit örtlichen Mitteln bewältigt werden, kann von einer Behörde eine Katastrophe ausgerufen werden.“[16]

Wesentlich ist, dass eine Katastrophe nur durch eine Behörde ausgerufen werden kann. Daher handelt es sich bis zur Deklaration durch eine Behörde um ein Krisenereignis.

11 URL: http://www.fremdwort.de/suche.php?term=Gefahr [08.12.2011].
12 URL: http://www.lfu.bayern.de/geologie/massenbewegungen/definition_gefahren/index.htm [08.12.2011].
13 Vgl. URL: http://www.duden.de/rechtschreibung/Interdependenz [22.12.2011].
14 „Gefahren und Interdependenzen“ URL: http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Gefahren/GefahrenBBK.html [05.01.12].
15 URL: http://www.ris.bka.gv.at/Dokumente/LrW/LRWI_B450_000/LRWI_B450_000.html
16 URL: http://www.springermedizin.at/artikel/15197-retten-was-zu-retten-ist [08.12.2011].

1.2.6 Krise und Krisenmanagement

Unter Krise versteht man „Eine vom Normalzustand abweichende, sich plötzlich oder schleichend entwickelnde Lage, die durch ein Risikopotenzial gekennzeichnet ist, das Gefahren und Schäden für Leib und Leben von Menschen, bedeutende Sachwerte, schwerwiegende Gefährdungen des politischen, sozialen oder wirtschaftlichen Systems in sich birgt und der Entscheidung – oftmals unter Unsicherheit und unvollständiger Information – bedarf.“[17]

Krisen sind mit der Standardorganisation nicht bewältigbar und erfordern zur Bewältigung außergewöhnliche Maßnahmen, wie z. B. den Einsatz von Krisenstäben. Darüber hinaus entsteht ein hohes öffentliches und mediales Interesse, welches heute besonders hohe Anforderungen an die Krisenkommunikation stellt.

Krisenmanagement bedeutet die „Schaffung von konzeptionellen, organisatorischen und verfahrensmäßigen Voraussetzungen, die eine schnellstmögliche Zurückführung der eingetretenen außergewöhnlichen Situation in den Normalzustand unterstützen.“[18]

„Erfolgreiches staatliches Krisenmanagement ist eine Leistung, die von einem Netzwerk von staatlichen und privaten Akteuren gemeinsam erbracht wird. Grundlage ist ein fachlicher Abstimmungsprozess zwischen Bund, Ländern, Wirtschaft, Wissenschaft und weiteren Kooperationspartnern.“[19]

Gesamtheitlich betrachtet bedeutet Krisenmanagement nicht nur die akute Begegnung einer Krise, sondern „alle Maßnahmen zur Vermeidung von, Vorbereitung auf, Erkennung und Bewältigung sowie Nachbereitung von Krisen“ (vgl. Abbildung 1).[20]

Abbildung 1: Notfall/ Katastrophenmanagementzyklus
Quelle: BBK

1.2.7 Krisenkommunikation

Krisenkommunikation fasst „Alle kommunikativen Aktivitäten, die in Zusammenhang mit einer Krise durchgeführt werden.“ zusammen. „In der Praxis bedeutet Krisenkommunikation die klare Zuordnung von Zuständigkeiten und Verantwortlichkeiten, sowie eine klare Kommunikationslinie für ein inhaltlich und argumentativ einheitliches Auftreten. Dazu bedarf es auch der Einigung darüber, wie die Medien bei der Aufarbeitung der Krise eingebunden werden sollen.“[21]

Vor allem bei einer Krise außergewöhnlichen Umfangs, mit weitreichenden Konsequenzen für die Bevölkerung und Gesellschaft, kommt einer professionellen Krisen-

17 Bundesministerium des Innern, 2005, S. 52.
18 Bundesministerium des Innern, 2005, S. 52.
19 „Grundlagen Krisenmanagement“ URL: http://www.bbk.bund.de/DE/AufgabenundAusstattung/Krisenmanagement/GrundlagenKrisenmanagement/grundlagenkrisenmanagement_node.html [09.12.2011].
20 http://www.bbk.bund.de/DE/Servicefunktionen/Glossar/_function/glossar.html?lv2=1899384&lv3=1956412
21 Bundesministerium des Innern, 2005, S. 52.

kommunikation ein außergewöhnlich hoher Stellenwert zu. Wie verschiedene Beispiele der jüngsten Vergangenheit zeigen, kann mit einer mangelhaften Krisenkommunikation sehr viel Schaden angerichtet werden.[22] Auf der anderen Seite wird auch eine professionelle Krisenkommunikation immer Ziel von Kritik sein, da sich die Menschen und Medien immer zu wenig informiert fühlen werden. Aufgrund des Wesens einer Krise – der fehlende Überblick über die Gesamtlage und das Fehlen von ausreichenden Informationen – wird auch professionelle Krisenkommunikation immer angreifbar bleiben. Entscheidend bleibt jedoch eine entsprechende Vorbereitung, eine einheitliche oder gemeinsame Stimme („Gesicht"), kompetentes Auftreten des Kommunikators und möglichst hohe Transparenz und Glaubwürdigkeit.[23]

1.2.8 Kritische Infrastruktur

Siehe strategische Infrastruktur.

1.2.9 Risiko und Risikomanagement

„Im allgemeinen Sinne versteht man unter **Risiko** die Wahrscheinlichkeit, mit der aus einem Zustand oder Vorgang ein Ereignis mit negativer Wirkung – ein Schaden – entstehen kann. Im engeren Sinne gibt das Risiko die qualitative und quantitative Charakterisierung eines möglichen Schadens an. Es beschreibt insbesondere die Tragweite der Schadenswirkung und kann durch das Produkt aus Eintrittswahrscheinlichkeit und Schadensausmaß beziffert werden."[24]

„Von **Risiko** spricht man nur, wenn die Folgen ungewiss sind; ein sicherer Verlust ist kein Risiko. Meist ist Risiko mit einer menschlichen Handlung verbunden, oft, aber nicht zwingend, im Sinne eines bewusst eingegangen, kalkulierten Risikos."[25]

„Die **Risikoerwartung** wird abgestuft dargestellt und mit „sehr hoch", „hoch", „mittel", „niedrig", „gering" und „sehr gering" bezeichnet."[26]

„Gefährdungs- und Risikoanalysen sind der Ausgangspunkt und ein zentraler Bestandteil des integralen **Risikomanagements**. Darunter versteht man das systematische Identifizieren, Bewerten und Priorisieren von Gefährdungen und deren Risiken, sowie das Steuern von Maßnahmen zur Risikominderung. Die einzelnen Phasen Vorbeugung, Bewältigung und Regeneration, sind im

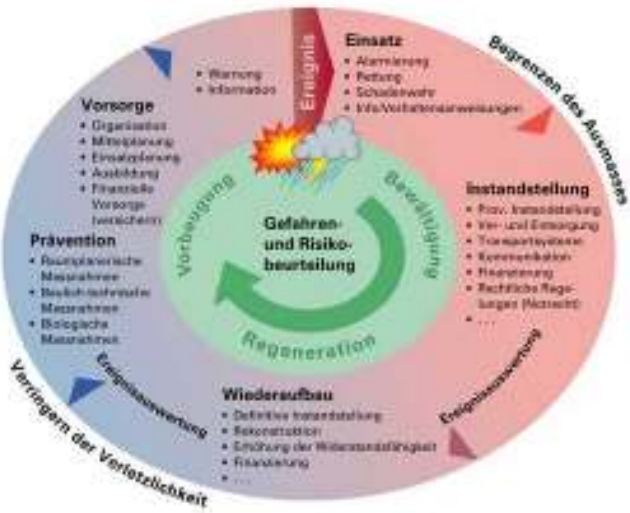

Abbildung 2: Kreislauf des integralen Risikomanagement
Quelle: Bundesamt für Bevölkerungsschutz (CHE)

22 Vgl. Krisenkommunikation im Rahmen der Ölkatastrophe im Golf von Mexiko, der Atomkatastrophe von Japan, oder der Ausbruch der EHEC-Epidemie in Deutschland.

23 Vgl. Freie Universität Berlin, 2011, S. 6.

24 „Risiko / Restrisiko" URL: http://www.lfu.bayern.de/geologie/massenbewegungen/definition_gefahren/doc/risiko.pdf [08.12.2011].

25 Der Große Brockhaus, 2010, (zit. nach Witzer, 2011, S. 45).

26 Bundesministerium des Innern, 2005, S. 52f.

Modell des integralen Risikomanagements gleichwertig und beeinflussen sich gegenseitig. Die Abgrenzung der Phasen ist fließend“ (vgl. Abbildung 2).[27]

Es gibt zwischen Risiko- und Krisenmanagement starke Parallelen.

1.2.10 Resilienz

Die Resilienz bezeichnet die Fähigkeit eines Systems, trotz externer Einflüsse, stabil zu bleiben. Oft wird Resilienz auch mit den Begriffen „Widerstandsfähigkeit“ oder „Robustheit“ in Verbindung gebracht.[28] Dieser Begriff hängt eng mit der Überlebensfähigkeit im Sinne der Kybernetik zusammen.[29]

1.2.11 Restrisiko

„Als **Restrisiko** wird die Gefährdung bezeichnet, die einem (technischen oder natürlichen) Prozess nach dem Stand der Wissenschaft selbst bei Anwendung aller theoretisch möglichen Sicherheitsvorkehrungen noch anhaftet (wissenschaftlich denkbare Vorkehrungen). Da der Stand der Wissenschaft dem technischen Stand immer voraus eilt, wird bei besonders sicherheitsrelevanten Prozessen die Formulierung Stand der Wissenschaft und Technik – (technisch denkbare Vorkehrungen) und bei weniger gefährlichen Prozessen – Stand der Technik – (technisch machbare Vorkehrungen) verwendet.“[30]

Dass die Aussagen zum Restrisiko ein zweischneidiges Schwert sind, beweisen einmal mehr die bisherigen Atomkatastrophen. Die 1989 von der Gesellschaft für Reaktorsicherheit vorgelegte Studie kam zum Schluss, dass schwere Unfälle mit radioaktiver Belastung der Umwelt nur alle 33.000 Reaktorjahre zu erwarten seien.[31] Auf den ersten Blick kann durchaus ein falscher Eindruck entstehen, vor allem, wenn nicht berücksichtigt wird, dass ein solches Ereignis auch sofort eintreten kann. Die Geschichte hat diesen möglichen Trugschluss mittlerweile mehrfach widerlegt. In Anbetracht der Atomkatastrophe von Japan, kann man daher das Restrisiko auch etwas zynisch sehen.

Abbildung 3: Ein Bild sagt mehr als tausend Worte. Quelle: www.badische-zeitung.de und http://de.toonpool.com/ 1

27 URL: „Mit Gefährdungen und Risiken umgehen“ http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/gefaehrdungen-risiken.html [09.12.2011].

28 Vgl. „Resilienz“ URL: http://wirtschaftslexikon.gabler.de/Archiv/255105/resilienz-v2.html [16.12.2011].

29 Siehe auch Abschnitt 2.3.1 Überlebensfähigkeit.

30 ebenda.

31 Vgl. „Umweltlexikon-online.de: GAU“ http://www.umweltlexikon-online.de/RUBsonstiges/GAU.php [10.12.2011].

1.2.12 Strategische Infrastruktur

„Zu den kritischen/strategischen Infrastrukturen zählen jene Infrastrukturen oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche oder soziale Wohl der Bevölkerung oder die effektive Funktionsweise von Regierungen haben."

Dazu zählen etwa Infrastrukturen aus den Bereichen Energieversorgung, Telekommunikation, Finanz-, Gesundheits-, Ver- und Entsorgungs- sowie Transportwesen, aber auch der öffentlichen Sicherheit. International wird dafür häufig der Begriff „Kritische Infrastruktur/Critical Infrastructur" verwendet.[32]

„Unsere Probleme sind das Resultat überholter Denkweisen.
Wir können diese Probleme nicht mit denselben Denkweisen lösen,
durch die sie entstanden sind."

A. Einstein

32 Vgl. Bundeskanzleramt, 2008.

2 Komplexe Systeme und die Stromversorgung

In unserer hoch vernetzten und vielseitig abhängigen Welt wird immer wieder der Begriff komplexe Systeme verwendet. Dieser Begriff trifft mittlerweile auch für unsere Stromversorgung zu. Daher erfolgt hier eine kurze Auseinandersetzung mit komplexen Systemen und den Grundzügen der Kybernetik[33], sowie den Wechselwirkungen in der Stromversorgung.

> *„Unter Kybernetik (vom griechischen kybernetes, der Steuermann) versteht man die Erkennung, Steuerung und selbsttätige Regelung ineinander übergreifender, vernetzter Abläufe bei minimalem Energieaufwand."*[34]

> *„Das fundamentale Prinzip kybernetischen Denkens ist, so meine ich, die Idee der Zirkularität."*[35]

2.1 Systeme

Wie so oft gibt es auch für ein System keine allgemein gültige Definition. In dieser Arbeit wird daher unter einem System ein Gebilde aus Einzelelementen bzw. Variablen verstanden, welches über eine Abgrenzung zu anderen Systemen verfügt und mit anderen Systemen in Wechselbeziehung steht. Die einzelnen Elemente verstärken oder schwächen andere Elemente des Systems in Form von Rückkopplungen.[36]

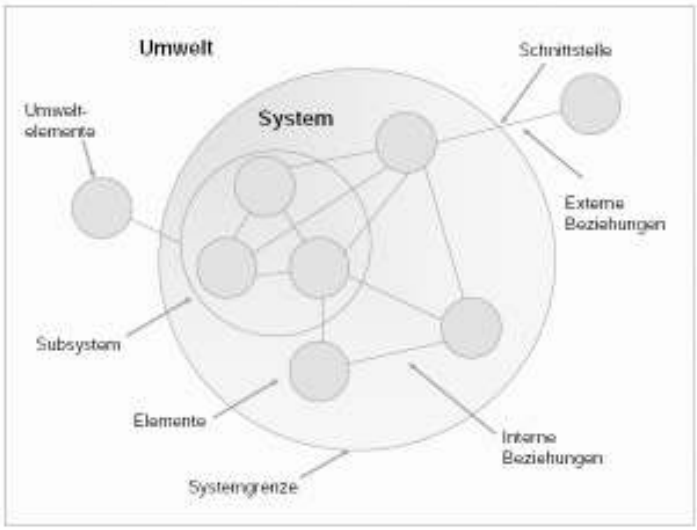

Abbildung 4: Grundbegriffe zur Systemdefinition
Quelle: Schulte-Zurhausen (Organisation, 2002), S. 34

Zum besseren Verständnis ein konkretes Beispiel:

> *„Was ist der Unterschied zwischen einem Haufen Sand und einer Blume? Sind beide ein System? Warum nicht?*
> *Ein Haufen Sand ist kein System: man kann Teile davon vertauschen, eine Handvoll wegnehmen oder dazutun es bleibt ein Haufen Sand. Eine Blume hingegen ist ein System: sie besteht aus mehreren verschiedenen Teilen.*
> *Zweite wichtige Eigenschaft eines Systems ist: die einzelnen Teile sind in einem bestimmten Aufbau miteinander vernetzt: Ein System verhält sich völlig anders als seine Teile. Es wird zu einem neuen Ganzen und das ist immer mehr als die Summe der einzelnen Teile oder Sub-Systeme."*[37]

33 Vom englischen Begriff „cybernetics" wurde auch der heute geläufige Begriff „Cyber..." abgeleitet.
34 Vester, 2011, S. 154.
35 Foerster, 2011, S. 106.
36 Vgl. Vester, 2011, S. 15ff.
37 URL: http://www.wimmer-partner.at/pdf.dateien/syst-denk.pdf [16.12.2011].

2.2 Lineare Systeme

Lineare (triviale) Systeme zeichnen sich durch eine klare und nachvollziehbare Strukturierung aus. Der Handlungsablauf erfolgt in Serie, eins nach dem anderen. Die Anzahl der Vorgänge spielt dabei keine Rolle. Das Verhalten ist reversibel und wiederholbar.[38]

> *„Eine triviale Maschine* (Anm.: System) *ist durch eine eineindeutige Beziehung zwischen ihrem 'Input' (Stimulus, Ursache) und ihrem 'Output' (Reaktion, Wirkung) charakterisiert. Diese invariante Beziehung ist 'die Maschine'. Da diese Beziehung ein für allemal festgelegt ist, handelt es sich hier um ein deterministisches System; und da ein einmal beobachteter Output für einen bestimmten Input für den gleichen Input zu späterer Zeit ebenfalls gleich sein wird, handelt es sich dabei auch um ein vorhersagbares System."*[39]

Zum Beispiel liefert eine mathematische Kalkulation bei Verwendung der selben Variablen immer das gleiche Ergebnis.

2.3 Komplexe Systeme

Die Komplexität bzw. „Undurchschaubarkeit" von Systemen entsteht erst durch Vernetzung. Dabei hängt die Komplexität des Gesamtsystems wesentlich vom Umfang der Vernetzung ab bzw. steigt mit dieser. Für den Vernetzungsgrad, und der damit steigenden Komplexität, spielt der stetig steigende Einsatz von Informations- und Kommunikationstechnologien eine ganz wesentliche Rolle. Oftmals wird diese auch durch eine unreflektierte Anwendung des Wachstumsparadigmas vorangetrieben.

Wesentlich ist, dass sich komplexe Systeme durch ihre nicht linearen Wirkungsbeziehungen zu anderen Systemen auszeichnen. Indirekte Wirkungen, Beziehungsnetze und Zeitverzögerungen verhindern häufig eine Zuordnung der Ursachen, was eine Folgenabschätzung von Eingriffen erheblich erschwert.[40]

Ein wesentlicher Unterschied zu linearen Systemen ist die ständige Rückkoppelung der Variablen („Zirkularität"), womit Ursache gleich Wirkung und umgekehrt ist. Als Beispiel für diese Zirkularität kann ein Heizungssystem mit Thermostat herangezogen werden. Sinkt die Raumtemperatur ab, schaltet das Thermostat die Heizung ein. Wird die gewünschte Temperatur erreicht, wird die Heizung durch das Thermostat wieder abgeschaltet. Die Variablen beeinflussen sich gegenseitig.

2.3.1 Überlebensfähigkeit

Komplexe Systeme sind immer mehr als die Summe ihrer Einzelteile. Eine wesentliche Unterstützung bei der Betrachtung von komplexen Systemen ist die Analogie zu den Funktionen von Organismen. Hier sind nicht perfekte Details, sondern das Zusammenspiel aller Elemente, für die Überlebensfähigkeit („Resilienz") entscheidend.[41]

Das systemrelevante Hauptziel ist die Erhöhung und Sicherung der Lebens- und damit Überlebensfähigkeit des Systems. Aus der Biologie wissen wir, dass sich langfristig nur jene Organismen durchsetzen und überleben konnten, welche sich an die Umfeldbe-

38 Vgl. Renn, Ortwin: *Normale Katastrophen nach Perrow.* In: Internet, unter URL: http://soz.fsen.faveve.uni-stuttgart.de/inhalte/scripte/technikundumwelt/Technik_Umwelt.pdf [16.12.2011].

39 Foerster, Heinz von: *Wissen und Gewissen: Versuch einer Brücke.* Berlin: Suhrkamp Verlag, S. 206f.

40 Vgl. Vester, 2011, S. 15f.

41 Vgl. ebenda, S. 25ff.

dingungen angepasst und vor allem Lösungen entwickelten haben, ihren Energiebedarf zu reduzieren. Durch die Reduktion des Energiebedarfs wurde die Abhängigkeit von der Umwelt reduziert und somit die Überlebensfähigkeit erhöht.[42]

Eine Erkenntnis, die sich unmittelbar in unserem Energiekonsumverhalten niederschlagen sollte. Die Realität ist aber weit davon entfernt. Es wurde zwar erkannt, dass neue Energieformen zur Stillung unseres unersättlichen Bedarfs erforderlich sind, aber der Fokus scheint nach wie vor in die falsche Richtung zu gehen. Die medial wahrnehmbaren Intentionen gehen vor allem in den weiteren Ausbau von Anlagen und in großflächige Vernetzungen.[43] Ob das zur Stabilisierung, oder doch eher zu mehr Abhängigkeit und Verwundbarkeit („Vulnerabilität“) führt, wird erst die Zukunft zeigen. Einige Aspekte bzw. Systemzusammenhänge der europäischen Stromversorgung werden noch im Kapitel Stromversorgungssicherheit näher analysiert.

Um die langfristige Stabilität und Überlebensfähigkeit der Stromversorgungssysteme und damit unserer Lebensgrundlage zu sichern, sollte unser Fokus auf die Reduktion des Energiebedarfs und nicht auf den weiteren Ausbau gerichtet werden. Um dieses Ziel zu erreichen, sind noch massive Anstrengungen und eine aktive Einbindung der Bevölkerung erforderlich. Einzelmaßnahmen, wie das eher fragwürdige Glühbirnenverbot, oder konkrete Schritte gegen den Stand-by Verbrauch, werden dabei bei Weitem nicht ausreichen. Ohne Entwicklung von neuen Wegen und Technologien wird dieses Ziel nur schwer zu erreichen sein.

2.3.2 Fehlertoleranz

Ein wesentlicher Faktor für die Überlebensfähigkeit eines Systems ist die Fehlertoleranz, die Robustheit („Resilienz“) gegenüber Störungen und Schwankungen in seinem Umfeld.

Wir müssen immer häufiger die Folgen der Missachtung dieses Faktors beobachten. Eine wesentliche Rolle dabei spielt die steigende und wenig fehlertolerante Technisierung, wodurch weitere Fehlerquellen geschaffen werden. Beispielhaft sei hier ein durch Computerprogramme ausgelöster Börsenabsturz[44] oder ein schwerer Zwischenfall mit einem Airbus[45], ausgelöst durch einen Softwarefehler, angeführt. Auch die Ausgrenzung von Systemteilnehmern, wie etwa die völlige Entkoppelung der Finanzwirtschaft von der Realwirtschaft oder die Konzentration auf eine einzige Führungsgröße, dem Bruttoinlandsprodukt (BIP), sind weitere Beispiele von vielen.[46]

Eine bereits etwas ältere Analyse verschiedener Katastrophen kommt zum Schluss, dass die mangelhafte Fehlerfreundlichkeit von Systemen trotz, wenn nicht sogar we-

42 Vgl. ebenda, S. 49f.

43 Vgl. u. a. URL: http://www.desertec.org [26.05.2011].

44 Vgl. „Der Börsencrash von Vancouver“ URL: http://www.dradio.de/dlf/sendungen/forschak/795396/ [29.12.2011].

45 Vgl. „Qantas flight terror blamed on computer“ URL: http://www.smh.com.au/travel/travel-incidents/qantas-flight-terror-blamed-on-computer-20111219-1p1to.html [29.12.2011].

46 Vgl. Vester, 2011, S. 30ff.

gen der hohen Sicherheitstechnik, ausgelöst wurde.[47] [48] Im Kapitel Krisen- und Katastrophenereignisse werden aktuelle Bestätigungen dieser Aussage zu finden sein.

Zum besseren Verständnis kann der Bahnverkehr herangezogen werden. Die Zeitersparnis für das Gesamtsystem, den Großteil der Reisenden, wird nicht durch die Fokussierung auf die Zeitersparnis bei einzelnen Zügen erreicht, sondern durch eine gesamtheitliche Betrachtung und das Einkalkulieren von entsprechenden Reserven auf den Einzelstrecken. Ein entsprechender Zeitpuffer (=Fehlertoleranz) ermöglicht das Ausgleichen von unvorhergesehenen Ereignissen. Dadurch können in der Regel Reisende die Anschlussverbindungen rechtzeitig erreichen. Ganzheitlich betrachtet ergibt sich dadurch eine weit höhere Zeitersparnis, als wenn bei jeder kleinen Störung längere Wartezeiten auf die nächste Anschlussverbindung in Kauf genommen werden müssen. Nicht das Einzelereignis ist wichtig, sondern das Gesamtsystem. Die Kundenzufriedenheit steigt durch die Gesamtpünktlichkeit und nicht durch die Einsparung von wenigen Minuten bei gleichzeitigem Risiko, länger Wartezeiten in Kauf nehmen zu müssen. Exakte Planung verlangt den Ausschluss von Fehlern und das widerspricht unserer Natur.[49]

2.3.3 Wachstum und Vernetzung

Unser derzeitiges Gesellschaftssystem und unser Wohlstand sind auf ständiges Wachstum („Wachstumsparadigma“) ausgerichtet. Vor allem unser Wirtschaftssystem hängt völlig von diesem Faktor ab. Mittlerweile verdichten sich die Anzeichen, dass dieses System in dieser Form nicht weiter funktionieren wird und in der Sackgasse steckt.

In einem Vergleich mit der Biologie könnte durchaus die Analogie zu einem Tumor gefunden werden. In der ersten Phase ist er auch sehr erfolgreich und das Konzept bewährt sich. Langfristig und in letzter Konsequenz führt dieses unkontrollierte Verhalten jedoch zur Selbstzerstörung.[50]

Auch nach der Finanzkrise 2008 wurden weitgehend nur oberflächliche Maßnahmen veranlasst und vor allem schlechtes Management belohnt. Kranke Unternehmen, in diesem Fall Banken, wurden durch hohe Subventionen künstlich wettbewerbsfähig gehalten. Zusätzlich wurden enorme Subventionen in Großprojekte gesteckt, um vermeintlich Arbeitsplätze zu schaffen. Dies mag zwar kurzfristig stimmen, viele Projekte, vor allem Bauprojekte, sind aber nicht auf die nachhaltige Schaffung von Arbeitsplätzen ausgerichtet.[51]

Nun könnte entgegnet werden, dass die Allgemeinheit so gut wie nie zuvor lebt, was kurzfristig auch schwer zu widerlegen ist. Den wenigsten Menschen ist aber bewusst, dass dieser Standard vor allem auf ungedeckten Schecks beruht. Veränderungen in komplexen Systemen wirken sich in der Regel langfristig aus, die Wirkung ist deutlich zeitverzögert. Zum Beispiel haben sich die Schadensbilanzen aus Umweltkatastrophen

47 Vgl. Perrow, Charles: *Normale Katastrophen: Die unvermeidbaren Risiken der Großtechnik.* Campus Verlag, 1992[2]

48 Vgl. Vester, 2011, S. 43.

49 Vgl. ebenda, S. 43ff.

50 Vgl. Vester, 2011, S. 70.

51 Vgl. ebenda, S. 66.

seit den achtziger Jahren des letzten Jahrhunderts vervielfacht. Die ersten Berichte gehen davon aus, dass 2011 das Jahr der höchsten Schäden aus Naturkatastrophen aller Zeiten sein wird. Ein gesamtwirtschaftlicher Schaden von rund 292 Milliarden Euro, das sind fast zwei Drittel mehr als der bisherige Höchststand aus dem Jahr 2005, wird erwartet.[52] Dennoch ist es menschlich, dass wir uns keine Veränderungen und schon gar nicht solche, die ein Umdenken verlangen oder zur Aufgabe eingespielter Verhaltensmuster zwingen, wünschen.[53]

Was hat das alles mit der Stromversorgung zu tun? Die bisherige, mehr oder weniger Monopolstellung der Energieversorgungsunternehmen, häufig in öffentlicher Hand, war wohl ein zusätzlicher Grund dafür, dass alternative Entwicklungen, wie kleinräumige Verbundlösungen, Rückspeisungen ins Netz oder die Nutzung von Industrieabwärme nicht unbedingt gefördert wurden.[54] Die derzeitigen Umbrüche, die relativ rasch vonstatten gehen, wurden aber im bisherigen Gesamtsystem kaum berücksichtigt. Daher sind die Folgen der derzeitigen Eingriffe noch nicht absehbar.[55] Auf der anderen Seite sind auch Energieversorgungsunternehmen Wirtschaftsunternehmen, die dem derzeitigen Wachstumsparadigma, folgen (müssen). Daher sollten Initiativen, wie etwa der beabsichtigte, massive Netzausbau in Europa oder die Errichtung von großen solarthermischen Kraftwerken in der Wüste,[56] sowie die Einführung von intelligenten Stromzählern[57] durchaus kritisch hinterfragt werden. Dies vor allem, wenn nur positive Begründungen vorliegen. Dass derartige Entwicklungen nicht immer zur Überlebensfähigkeit des Gesamtsystems beitragen müssen, wird in dieser Arbeit noch näher beleuchtet.

Ein nicht vernetztes System ist nicht stabil, da es auf sich alleine gestellt ist. Mit der wachsenden Vernetzung steigt die Stabilität, jedoch nur bis zu einem bestimmten Grad. Ab einem bestimmten Vernetzungsgrad sinkt diese wieder. Neu gebildete Unterstrukturen können wieder, bei gleichzeitig hoher Vernetzung, zur Stabilisierung und Erhöhung der Überlebensfähigkeit des Systems beitragen (siehe auch Abbildung 4, Seite 14).[58]

Die Bildung dieser Untersysteme hat mehrere, notwendige Konsequenzen:[59]

1. Die Anzahl der erforderlichen Kommunikationsvorgänge zwischen den einzelnen Elementen wird reduziert.
2. Die einzelnen Elemente in den Untersystemen können sich auf ihre Teilaufgabe spezialisieren und diese damit deutlich besser erfüllen.
3. Die Steuerung und Kommunikation zwischen diesen Untersystemen wird für das Funktionieren des Gesamtsystems überlebenswichtig. Je komplexer diese Untersysteme sind, desto wichtiger und aufwendiger wird die Integration des Gesamtsystems.

52 Vgl. „380 Mrd. Dollar Schaden durch Naturkatastrophen“ URL: http://news.orf.at/stories/2097848/ [04.01.2012].
53 Vgl. Vester, 2011, S. 75f.
54 Vgl. ebenda, S. 52.
55 Vgl. auch ab Abschnitt 4.2.4, Intelligente Stromnetze
56 Vgl. URL: http://www.desertec.org [17.12.2011].
57 siehe auch Abschnitt 4.2.5 Intelligente Stromzähler
58 Vgl. Vester, 2011, S. 68ff.
59 Vgl. Dorn, 2004, S. 4.

4. Durch diese Untergliederung werden die Verhaltensmöglichkeiten der Untersysteme und der Elemente deutlich eingeschränkt.
5. Durch diese Strukturierung steigt die Komplexität des Gesamtsystems. Dadurch verändert sich auch ein lineares Verhalten zu einem zirkularen. Ursache und Wirkung sind nicht mehr einfach zuordenbar. Einzelne Ergebnisse sind daher nicht mehr vorhersagbar.

2.3.4 Kontraproduktiver Aktionismus

Im generellen steigt das Bewusstsein für die Notwendigkeit von ganzheitlichen Betrachtungen von Entscheidungsfindungen in der Politik, Wirtschaft, Finanzwelt oder Verwaltung. Dennoch gibt es noch genügend Beispiele für isolierte Behandlungen von Einzelbereichen, die wohl auf eine gewisse Hilflosigkeit und ständigen Zeitdruck zurückzuführen sind. Dieses Manko ist auch auf die fehlende Ausbildung im Umgang mit diesen Herausforderungen zu suchen. Vor allem bedeutet ein mehr an Informationen nicht, auch besser informiert zu sein und bessere Entscheidungen treffen zu können. Ganz im Gegenteil, es verleitet dazu, sich in Details zu verlieren.[60]

Zur Verdeutlichung kann die Funktion unseres Gehirns herangezogen werden, dessen Aufgabe es ist, die permanenten und umfangreichen Wahrnehmungen der Sinnesorgane (etwa Augen, Ohren, Haut, Nase) möglichst stark und auf das Notwendigste zu reduzieren.

Entscheidungsträger sehen sich häufig, besonders durch medialen Druck, dazu veranlasst, Probleme dort zu bekämpfen, wo sie auftreten (z. B. „Anlassgesetzgebung“). In einem komplexen System führt jedoch die Beseitigung eines Problems ohne einer entsprechenden Systembetrachtung meist zu der Schaffung von neuen Problemen. Hier sind wohl jedem eine Vielzahl an Beispielen aus dem Alltag bekannt.

Als Negativbeispiel kann die geplante Einführung von intelligenten Stromzählern („Smart Meter“) angeführt werden.[61] In Österreich wurde das entsprechende Gesetz[62] ohne großes Aufsehen durch zwei Drittel der Abgeordneten des Nationalrates durchgewunken. Eine ähnliche Vorgehensweise erfolgte bei der Umsetzung der dazugehörigen Verordnung für die technischen Mindestanforderungen von intelligenten Messgeräten im Sommer 2011. Erhebliche Bedenken wurden negiert und die Verordnung im Eiltempo erlassen.[63] Bei Bedarf soll es Zusatzverordnungen geben, die wahrscheinlich in einem Flickwerk enden und erhebliche Mehrkosten verursachen werden.[64] Fast alle Aussagen beziehen sich auf das nicht wirklich belegte Stromeinsparpotential und den positiven Nutzen für die Kunden.[65] Alleine die Tatsache, dass den Entscheidungsträgern quasi nur Vorteile präsentiert wurden, hätte Misstrauen erzeugen müssen. Be-

60 Vgl. Vester, 2011, S. 15f.
61 Vgl. Saurugg, 2011, 2011b.
62 Novellierung des Elektrizitätswirtschaftsund Organisationsgesetz (ElWOG) im Dezember 2010.
63 Vgl. „IMA-VO Begutachtung“ URL: http://www.cybersecurityaustria.at/CSA/HOME_files/Stellungsnahme_Smartmeter_IVO_v5.pdf [16.12.2011].
64 Vgl. „Versorgungssicherheit durch "Smart Meter"-Verordnung der E-Control gefährdet!“ URL: http://www.pressetext.com/news/20111104016 [16.12.2011].
65 Vgl. „Mitterlehner schickt neue Smart-Meter-Verordnung in Begutachtung“ URL: http://www.bmwfj.gv.at/Presse/AktuellePressemeldungen/Seiten/smartmeter.aspx [29.12.2011].

sonders, nachdem sich in den vergangenen Jahren die (Sicherheits-)Probleme in der IT-Welt vervielfacht haben. Beim intelligenten Stromzähler handelt es sich letztendlich um einen Computer. Eine tiefer gehende Analyse wurde in der Seminararbeit *„Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit“*[66] durchgeführt.

2.4 Zusammenfassung

In diesem Kapitel wurde versucht, die Grundzüge der Kybernetik näher zu bringen.

Eine ausführliche Betrachtung der Kybernetik ist in dieser Arbeit nicht möglich, wenngleich diese für eine gesamtheitliche Krisenprävention, in diesem Fall beim Thema Stromversorgungssicherheit, unerlässlich scheint. Daher wird das Buch von Frederic Vester, „Die Kunst vernetzt zu denken, Ideen und Werkzeuge für einen neuen Umgang mit Komplexität“,[67] zur Vertiefung empfohlen. Die Kunst, vernetzt zu denken, sollte Bestandteil jeder Führungs- und Managementausbildung, sowie Technikfolgeabschätzung bzw. im Risikomanagement, sein.

Zusammenfassend sollen folgende wichtige Erkenntnisse aus diesem Kapitel für die weiteren Betrachtungen mitgenommen werden:

- Der Vernetzungsgrad bestimmt ganz wesentlich die Komplexität eines Systems.
- Je komplexer ein System, desto weniger kann sein Verhalten vorhergesagt werden. Eingriffe sind daher besonders behutsam vorzunehmen.
- Eingriffe in ein komplexes System wirken sich nicht unmittelbar und nicht linear aus. Dabei müssen vor allem mögliche Fern-, Neben- und Rückkopplungseffekte beachtet werden.
- Systeme sind langfristig nur überlebensfähig, wenn es ihnen gelingt, ihren Energiebedarf bestmöglich zu minimieren und optimieren.
- Störungen und Fehler an einer Stelle des Systems sollen sich möglichst nicht automatisch auf alle anderen Systemelemente übertragen.

Generelle Kennzeichen komplexer Handlungssituationen sind:[68]

- Komplexität
- Intransparenz
- Dynamik
- (Hoher) Vernetzungsgrad
- Unvollständige oder falsche Informationen über das jeweilige System

Besonders der Umgang mit unvollständigen und falschen Informationen sowie Hypothesen, stellen eine wichtige Herausforderung im Umgang mit komplexen Situationen dar.[69]

Abschließend soll hier noch der Ökonom, Klaus Gretschmann, eh. Wirtschaftsberater des deutschen Kanzlers Gerhard Schröder und später Generaldirektor im Rat der EU, aus einem Presseinterview zitiert werden:

66 Saurugg, 2011, 2011b.
67 Vester, 2011.
68 Vgl. Dörner, 2011, S. 59.
69 Vgl. ebenda, S. 66.

„Was heute deutlich wird ist, dass die Vielzahl von warnenden Stimmen, die uns frühzeitig darauf hingewiesen hatten, dass viele Sachfragen der Währungsunion ungeklärt seien, nicht ausreichend Gehör fanden.

Ich befürchte, dass die europäische Politik möglicherweise die falsche Krise löst, indem sie auf der Basis falscher oder unzureichender Analysen nicht die richtigen Entscheidungen trifft.

Wenn man nun etwa sagt: Die Lösung liegt in einer Schuldenbremse für alle, darin also, dass alle Länder sparen müssen, dann übersieht man, dass es sich hierbei zwar um eine längerfristig notwendige, aber kurzfristig keineswegs hinreichende Bedingung handelt.“[70]

Diese Aussagen betreffen zwar das europäische Währungssystem, sie lassen sich aber auf viele andere komplexe Systeme umlegen. Sie enthalten Hinweise, die auch in Bezug auf den Umgang mit unserer Stromversorgungssicherheit und damit einhergehend mit dem Thema Blackout, als Warnung verstanden werden können.

„If you don`t manage issues, issues will manage you“, Robert L. Heath

70 Gretschmann: "Dann bleibt nur mehr die Bazooka" URL: http://diepresse.com/home/wirtschaft/eurokrise/715743/Gretschmann_Dann-bleibt-nur-mehr-die-Bazooka [17.12.2012].

3 Krisen- und Katastrophenereignisse

Im nachfolgenden Kapitel werden einige Beispiele analysiert, wo Zwischenfälle Krisen und Katastrophen in unterschiedlicher Qualität und Quantität ausgelöst haben. Dabei soll besonders die Rolle einzelner Faktoren für das Gesamtgeschehen herausgearbeitet werden. Ziel ist die Darstellung der Abhängigkeiten und der Komplexität, in der sich einzelne Faktoren entscheidend auf das Gesamtsystem ausgewirkt haben. Damit soll einmal mehr vor Augen geführt werden, wie schnell und überraschend Unmögliches und Unvorstellbares dennoch möglich wird.

3.1 Deepwater Horizon – 2010

Am 20.April 2010 löste eine Kette von Ereignissen eine der größten Umweltkatastrophen der Geschichte aus. Die Explosion auf der Explorations-Ölbohrplattform Deepwater Horizon im Golf von Mexiko kostete 11 Menschen das Leben und verursachte in der Region eine verheerende Ölpest.

Bis zu diesem Zeitpunkt war die Explorations-Ölbohrplattform Deepwater Horizon durch positive Schlagzeilen, wie „weltweit tiefste Bohrung ihrer Art bis in eine Tiefe von 10.685 Meter“[71] oder die Auszeichnung mit dem „Safety Award for Excellence – outstanding drilling operations – perfect performance period“[72] 2009, bekannt geworden.

Durch die hohe Brisanz und die unvorstellbaren Schäden wurde nach der Katastrophe vom US-Kongress eine Untersuchung beauftragt. Diese kam zum Ergebnis, dass eine Vielzahl menschlicher und technischer Fehler zum Untergang der Bohrinsel und somit zur folgenschweren Umweltkatastrophe geführt haben.[73]

Wesentliche Erkenntnisse aus dem Untersuchungsbericht: Die Ölpest im Golf von Mexiko war die Folge von vermeidbaren Fehlern der an der Bohrung beteiligten Unternehmen und Aufsichtsbehörden.

3.1.1 Fehlentscheidungen

- Die Fehler resultierten zumeist aus Fehlentscheidungen der Firmen, mit denen Zeit- und Kosten eingespart werden sollten.
- Es wurde eine Reihe von gefährlichen und zeitsparenden Schritten getätigt, ohne die Risiken in Betracht zu ziehen.
- Sicherheitseinrichtungen (etwa Brandmeldeanlagen) wurden abgeschaltet, damit die Arbeiter nicht durch Fehlalarme gestört werden.
- Vorangegangene Warnhinweise wurden ignoriert.
- Übersteigende und gefährliche Selbstsicherheit entstanden durch die bisherigen Erfolge.
- Vertreter der Unternehmen haben vor kritischen Entscheidungen nicht genügend miteinander kommuniziert.

71 Vgl. „BP drills oil discovery in the Gulf of Mexico“ URL: http://www.offshore-mag.com/index/article-display/7488119241/articles/offshore/drilling-completion/us-gulf-of-mexico/2009/08/bp-drills giant .html [01.12.2011].

72 Vgl. „GoM Rig Teams Win MMS District SAFE Award, Transocean Nominated for National SAFE Award“ URL: http://www.beaconmag.com/gomrigteamswinmm.html [01.12.2011].

73 National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, 2011.

3.1.2 Mangelhafte Krisenprävention und -reaktion

- Die staatlichen Aufsichtsbehörden kamen ihren Pflichten nicht nach.
- Es gab keine klare Aufgabentrennung im Katastrophenmanagement.
- Die Rechtslagen waren oft unklar.
- Mangelhafte Koordinierung zwischen öffentlichem und privatem (Firmen) Krisenmanagement.
- Kompetenzstreitigkeiten zwischen national- und bundesstaatlichen Krisenmanagementeinrichtungen.
- Austragung von Konflikten via Medien.
- Die Gesundheitseinrichtungen waren nicht auf eine derartige Katastrophe und deren Folgen für Gesundheit und Bevölkerung vorbereitet.
- Das Krisenmanagement war nicht vorbereitet – die Maßnahmen zur Abdichtung des Loches erfolgten im „trial and error" Prinzip.
- Es wurde zu viel Zeit bis zur Ausrufung der Krise verschwendet.

Zeit- und Kostendruck führten zur Katastrophe im Golf von Mexiko. Dies könne sich jederzeit wiederholen, stellt der Abschlussbericht fest. Ohne erhebliche Reformen, sowohl im Vorgehen der Industrie als auch bei der Regierungspolitik, könnte eine solche Katastrophe jederzeit wieder passieren. Krisenmanagement beruht auf dem Handeln vor der Krise!

Viele Punkte, die auch hier einfach auf andere Situationen umlegbar sind und gleichzeitig Warnung sein sollten. Der Punkt „Übersteigende und gefährliche Selbstsicherheit durch die bisherigen Erfolge" war etwa auch bei der Atomkatastrophe von Tschernobyl ein wesentlicher Auslösefaktor.[74]

3.2 EHEC-Epidemie – 2011

Im Mai 2011 brach in Deutschland eine EHEC[75]-Epidemie aus, die zu schweren Durchfallerkrankungen führt. Sie wurde durch einen extrem seltenen Stamm des Darmbakteriums Escherichia coli ausgelöst. In Folge der Epidemie starben 50 Menschen durch die Erkrankung, mehrere Hundert Menschen leiden an massiven Folgeschäden.[76] [77]

> ***Epidemie**: „(auch: Seuche) bezeichnet eine im überdurchschnittlichen Maße, örtlich und zeitlich begrenzt auftretende Infektionskrankheit. Epidemisch auftretende Krankheiten sind viele Tropenkrankheiten wie die Dengue, aber auch Cholera, Grippe, Typhus."*[78]
>
> ***Pandemie:** „Von Pandemie spricht man, wenn es sich um einen länderübergreifenden oder weltweiten Ausbruch einer Krankheit handelt. Die Pandemie macht an den Ländergrenzen oder an den Grenzen eines Kon-*

74 Vgl. Dörner, 2011, S47ff.
75 Enterohämorrhagische Escherichia coli
76 Vgl. „EHEC-Infektionen" URL: http://www.rki.de/cln_117/nn_196658/DE/Content/InfAZ/E/EHEC/EHEC.html?__nnn=true [09.12.2011].
77 Vgl. „EHEC-Folgen Das Gehirn erholt sich – meistens" URL: http://www.focus.de/gesundheit/ratgeber/verdauung/ehec/ehec-folgen-das-gehirn-erholt-sich-meistens_aid_634595.html [09.12.2011].
78 „Lexikon: Gesetzliche Krankenversicherung"URL: http://www.cecu.de/590+M5150003c28d.html [09.12.2011].

> *tinents nicht Halt. Auch bei Pandemien gibt es Gebiete, die nicht von der Krankheit betroffen werden. Durch ihre geographische Lage können Gebiete von einer Infektion verschont bleiben."*[79]

Die hohe Anzahl von über 4.000 Patienten stellte in Europa bei dieser Erkrankung ein Novum dar.[80]

Trotz der umfangreichen Erfahrungen und Vorbereitungen auf eine mögliche Influenza-Pandemie in der Saison 2009/2010 kam es zu zahlreichen, teilweise schwerwiegenden Pannen,[81] die massive Kritik am Krisenmanagement[82] laut werden ließen.[83] Vor allem wurden mehrere Widersprüche aufgezeigt, wie etwa, dass trotz moderner Informations- und Kommunikationstechnik und vielschichtiger Vernetzungen, der Meldefluss völlig unzureichend war. Die Ausbreitung der Seuche wurde vor allem durch die umfangreichen Abhängigkeiten in der Lebensmittelversorgung begünstigt. Ganz wesentlich waren dabei die für Außenstehende oftmals völlig undurchsichtigen und komplexen Transportwege.

In diesem Fall spielten die heute einzigartigen und globalen Reisebewegungen bei der Ausbreitung der Seuche keine Rolle. In anderen Epidemie- oder Pandemieszenarien werden diese die Lage ganz wesentlich mitbestimmen. Ein ganz entscheidender Faktor ist dabei die Zeit. Lageerfassungen und Entscheidungen müssen in immer kürzeren Zeitabständen bewältigt werden.

Ein weiterer Faktor sind die Medien, die einen erheblichen Einfluss auf die öffentliche – und zum Teil irreführende – Wahrnehmung haben und damit auch falsche Entscheidungsgrundlagen liefern. Die Entscheidungsfindung wird damit beeinflusst, manchmal in die falsche Richtung.[84] Auch bei der EHEC-Epedemie wurde ein völlig verzerrtes Bild vermittelt. Dabei spielte sicher die Wortwahl, wie etwa „Killervirus", eine wichtige Rolle. Bei der EHEC-Epedemie verlief die Mehrzahl der Erkrankungen mild. 50 Todesopfer sind natürlich tragisch, aber bei der Influenza Pandemie gab es sogar mehr als 250 Todesopfer, ohne dass dies derart hochgespielt worden wäre.[85] Durch den fehlenden Realitätsbezug werden Dinge häufig schlimmer dargestellt, als sie in Relation zu anderen Risiken des täglichen Lebens, wie etwa beim Rauchen, sind. Begünstigt wurde dieser Missstand durch zahlreiche Pannen in der Krisenkommunikation, wie durch nicht abgestimmtes Vorgehen, abweichende Meinungen unter einer Vielzahl, auch selbsternannter, Experten und von kaum durchschaubaren Zuständigkeiten bei Bund und Ländern.[86]

79 „Lexikon: Gesetzliche Krankenversicherung" URL: http://www.cecu.de/590+M59360f2b52a.html [09.12.2011].

80 Vgl. Freie Universität Berlin, 2011, S. 7.

81 Vgl. „Lehre aus EHEC: Meldeweg wird verkürzt" URL: http://www.springermedizin.at/artikel/23326-lehre-aus-ehec-meldeweg-wird-verkuerzt [09.12.2011].

82 Vgl. EHEC-Krisenmanagement URL: http://www.stern.de/gesundheit/ehec-krisenmanagement-die-gurkentruppen-1692793.html [09.12.2011].

83 Vgl. Freie Universität Berlin, 2011, S. 11.

84 Ein besonders anschauliches Bild stellen die Untersuchungen zu den Folgen der Terroranschläge vom 11. September 2001 in den USA dar. Viele Amerikaner verzichteten in den darauf folgenden Monaten aus Furcht vor weiteren Anschlägen auf das Fliegen. Sie griffen stattdessen auf das Auto zurück. Die Folge war, dass es im Jahr nach den Anschlägen rund 1.500 Verkehrstote mehr gab, als sonst. Vgl. Freie Universität Berlin, 2011, S. 14.

85 Vgl. Freie Universität Berlin, 2011, S. 13.

86 Vgl. ebenda, S. 13f.

Interessant ist das Ergebnis einer Umfrage während der EHEC-Krise, welche die Zusammenhänge zwischen (Medien)Informationen / Wahrnehmung und dem angegebenen Verhalten der Bevölkerung verdeutlicht:

Demnach

- fühlten sich 50 Prozent der Befragten gut informiert,
- fanden über 70 Prozent der Befragten die Informationen verständlich aufbereitet waren,
- machten sich 25 Prozent der Befragten Sorgen oder sehr große Sorgen, unter den Frauen waren es sogar 33 Prozent,
- vermieden 50 Prozent der Befragten die entsprechenden Lebensmittel,
- veränderten 70 bis 80 Prozent der Befragten ihr Hygieneverhalten nicht!

Dass die Hälfte der befragten Menschen die angegebenen Lebensmittel mieden, war u. a. auf die erfolgreiche Krisenkommunikation zurückzuführen. Was aber auch fatale Folgen für einzelne Landwirtschaftsbereiche hatte, da die mögliche Gefahrenquelle mehrfach revidiert werden musste.[87] Anders sah die Umfrage bei der Handhygiene aus. Obwohl bekannt und wissenschaftlich belegt ist, dass das gründliche und mit Seife durchgeführtes Händewaschen wesentlich zum Schutz vor Infektionserkrankungen beiträgt, ist es nicht gelungen, eine entsprechende Verhaltensänderung herbeizuführen.[88]

Einen weiteren kritischen Punkt aus den Lessons Learned stellt die nachteilige Kompetenzzerstreuung dar. Für die EHEC-Krise waren verschiedenste Ressorts zuständig. Das Bundesministerium für Gesundheit (BMG), das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) sowie deren nachgeordnete Behörden, wie etwa das Bundesamt für Verbraucherschutz und Lebensmittelsicherheit (BVL), das Robert-Koch-Institut (RKI), das Paul-Ehrlich-Institut (PEI), die Bundeszentrale für gesundheitliche Aufklärung (BZgA). Der Föderalismus stellt bei derart komplexen und zeitlich kritischen Ereignissen ein massives Hemmnis dar. Besonders die unkoordinierte Krisenkommunikation verunsicherte die Bevölkerung zusätzlich.[89]

Auch aus diesem Beispiel können mehrere Lehren, insbesondere was die Krisenkommunikation und die Verantwortlichkeiten betreffen, unabhängig vom Szenario, mitgenommen werden.

3.3 Blackout Münsterland – 2005

2005 führt eine außergewöhnliche Wetterlage zu einem mehrtägigen Blackout für über 250.000 Menschen im dünn besiedelten Münsterland / Deutschland. Weitere Hintergrundinformationen werden zusätzlich im Abschnitt 4.1.4, Blackout 2005 – Deutschland, behandelt. Im folgenden Abschnitt werden einige Erkenntnisse aus einer Studie, die rund ein halbes Jahr nach dem Ereignis durch eine Befragung von Betroffenen Menschen erstellt wurde, zusammengefasst.

87 So standen alle mögliche pflanzliche Lebensmittel in Verdacht, wie Tomaten, Gurken, Salat bis schließlich Sprossen als Quelle des Keims identifiziert wurden.

88 Vgl. Freie Universität Berlin, 2011, S. 15.

89 Vgl. ebenda, S. 33.

Besonderheiten dieses Blackouts[90] [91]:

- Die Teilnehmer der Befragung waren im Durchschnitt drei bis vier Tage vom Stromausfall betroffen.
- Über 50 % der betroffenen Haushalte waren nicht in der Lage, in dieser Zeit zu heizen, über 40 % konnten kein Warmwasser erzeugen.
- Nur rund ein Drittel verfügte über eine Heizquelle, die ohne Strom auskam.
- Fast alle Haushalte hatten bei Beginn des Stromausfalls Lebensmittel zu Hause. Bei mehr als einem Drittel der Befragten hätten die Vorräte aber nur bis zu zwei Tagen gereicht, was in diesem Fall zu kurz gewesen wäre, hätte die Versorgung nicht funktioniert.
- Trotz Stromausfall wurden Supermärkte in der Region betrieben und auch am Sonntag geöffnet, womit die Versorgungslage nicht eskalierte.

Besonders erstaunlich war, dass trotz ländlichem Raum ein erheblicher Teil der Bevölkerung über keine ausreichende Eigenbevorratung verfügte, obwohl man dies gerade für einen solchen Raum noch am ehesten annehmen würde. Trotz dieser Rahmenbedingungen musste bei der Befragung festgestellt werden, dass sich das Einkaufsverhalten der Betroffenen wenige Monate nach dem Ereignis nicht wesentlich verändert hatte. Dies wurde darauf zurückgeführt, dass das Krisenmanagement während des Blackouts (zu) gut funktionierte und durch die Zufuhr von externer Hilfe (GOs und NGOs)[92] die Lebensmittelversorgung jederzeit sichergestellt werden konnte. Darüber hinaus wurden durch Hilfsorganisationen ausreichend Notverpflegsstellen eingerichtet. Indem aus dem gesamten Bundesgebiet Notstromaggregate herangeführt werden konnten, war es auch möglich, entsprechende Notstromversorgungsnetze aufzubauen.[93]

Alle diese außergewöhnlichen Rahmenbedingungen waren ausschlaggebend, dass sich aus der Großschadenslage keine Katastrophe entwickelte.[94]

Dieses Beispiel zeigt aber auch, dass es bei einer räumlich begrenzten Schadenslage durchaus möglich ist, durch das Heranführen von externen Ressourcen die allgemeine Situation relativ gut und rasch in den Griff zu bekommen. Leider lässt sie jedoch keine qualifizierten Rückschlüsse auf größere Ereignisse bzw. bei der Betroffenheit von größeren urbanen Gebieten zu. Eine wichtige Erkenntnis sollte sein, dass ein einmaliges Ereignis nicht wesentlich zu einer Verhaltensänderung der Bevölkerung im Sinne von Selbstschutz und -hilfe, beiträgt.

3.4 Wiener U-Bahn – Personenschaden – 2010

Im Mai 2010 wurde in Wien der Fuß eines fünfjährige Jungen zwischen den Türen einer abfahrenden U-Bahn eingezwickt. Der Junge wurde bis ans Ende des Bahnsteiges mitgeschleift und schwer verletzt. Er hatte versucht, mit seiner Mutter den abfahrenden Zug noch zu erreichen.[95]

90 Das Ergebnis bezieht sich auf die Rückmeldungen von rund 600 betroffenen Haushalten der am längsten betroffenen Ortschaften im Rahmen einer Umfrage. Es besteht dabei kein Anspruch auf Repräsentativität.

91 Vgl. Fachhochschule Münster, 2008, S. 67f.

92 (Non)Governmental Organisations wie, Bundeswehr, Technisches Hilfswerk (THW), Feuerwehren, Rotes Kreu, u.v.m.

93 Vgl. Fachhochschule Münster, 2008, S. 26.

94 Vgl. ebenda, S. 77.

Bei den Untersuchungen der technischen Einrichtungen wurden keine Fehler festgestellt. Daher wurde der U-Bahn-Fahrer als Schuldiger identifiziert und vom Dienst abgezogen.[96] Darüber hinaus bekam er eine Anzeige wegen fahrlässiger Körperverletzung.[97]

In weiterer Folge wurden 11 Millionen Euro investiert, um die U-Bahn-Züge noch sicherer zu machen.[98]

Eine erfolgreiche Krisenkommunikation? Auf den ersten Blick, ja. Dennoch muss hinterfragt werden – und das ist in der Öffentlichkeit nicht passiert – ob hier die richtigen Schlüsse gezogen wurden. Wie viel Eigenverantwortung kann den Bürgern zugemutet werden? Mittlerweile wurden zahlreiche U-Bahn-Türen mit Licht- und Tonsignalen ausgerüstet, die Durchsage geändert, neue Piktogramme eingeführt[99] und sehr viel Geld in die Hand genommen. Dennoch können fast täglich leichtsinnige und fahrlässige Fahrgäste beobachtet werden, die nach wie vor in abfahrende Züge springen und so sich selbst und andere gefährden. Es stellt sich daher die Frage, ob hier nicht mehr auf die Eigenverantwortung zu fokussieren ist. Die Gesellschaft kann es sich auf Dauer nicht leisten, jegliche Eigenverantwortung ihrer Bürger durch teure Absicherungsmaßnahmen zu kompensieren. Das muss stärker kommuniziert werden und spielt auch beim Thema Blackout eine nicht zu vernachlässigende Rolle. In diesem Fall hat es niemand öffentlich gewagt, die eigentlich verantwortungslose Mutter in die Pflicht zu nehmen, da ihr fahrlässiges Handeln für den Unfall ausschlaggebend war.

3.5 Terroranschläge auf öffentliche Verkehrsmittel in London – 2005

Im morgendlichen Stoßverkehr des 07.Juli 2005 explodierten vier Sprengsätze in vier verschiedenen Verkehrsmitteln des Londoner Nahverkehrs. 56 Menschen wurden dabei getötet und über 700 Menschen verletzt. [100]

Die Krisenreaktion der Behörden und der Bevölkerung ging in weiterer Folge als mustergültig ein. Dies wurde der professionellen und vor allem transparenten Krisenkommunikation zugeschrieben. Die Gefahr eines solchen Terroranschlags wurde zuvor über Jahre hinweg offen kommuniziert. Als die erwartete Krise tatsächlich eintrat, konnte die Krisenkommunikation auf diese ehrliche und offene Risikokommunikation aufbauen. Die Folge war, dass die Bevölkerung sehr ruhig und besonnen reagierte und in weiterer Folge den öffentlichen Nahverkehr weiter nutzte und kaum auf den Privatverkehr,

95 Vgl. „Fünfjähriger Bub von U-Bahn mitgeschleift“ URL: http://derstandard.at/1271376224007/U3-Station-Enkplatz-Fuenfjaehriger-Bub-von-U-Bahn-mitgeschleift [10.12.2011].

96 Vgl. „Wiener Linien treiben Untersuchungen nach U-Bahn-Unfall voran“ http://www.wienerlinien.at/eportal/ep/contentView.do/contentTypeId/1001/channelId/-8615/programId/22534/pageTypeId/9320/contentId/23672 [10.12.2011].

97 Vgl. „Menschliches Versagen wohl Unfallursache: U-Bahn-Fahrer übersah Frau und ihr Kind“ URL: http://www.news.at/articles/1018/10/268301/menschliches-versagen-unfallursache-u-bahn-fahrer-frau-kind [10.12.2011].

98 Vgl. „11 Millionen Euro Investition für mehr Sicherheit Schlupflöcher sollen geschlossen werden Umbau aller U-Bahn-Türen“ URL: http://www.wienerzeitung.at/themen_channel/wzwien/stadtleben/39325_Umbau-aller-U-Bahn-Tueren.html [10.12.2011].

99 Vgl. „Wiener U-Bahn mit neuen Sicherheitshinweisen“ URL: http://diepresse.com/home/panorama/wien/629735/Wiener-UBahn-mit-neuen-Sicherheitshinweisen [10.12.2011].

100 Vgl. „Terroranschläge am 7. Juli 2005 in London“ URL: http://www.spiegel.de/wikipedia/Terroranschläge_am_7._Juli_2005_in_London.html [10.12.2011].

anders als in den USA nach 9/11, umstieg. Der Londoner Raum hätte eine solche verkehrstechnische Situation überhaupt nicht verkraften können.[101]

Der damalige Anti-Terror-Chef gab fünf Jahre später zu Protokoll:

> *„Unsere Medienstrategie hat sicher geholfen. Das Allerwichtigste ist, dass die beteiligten Behörden dasselbe sagen. Zunächst geht es darum, zu beruhigen. (…) Das Wichtigste ist, zusammen zu planen und zu üben. Damit jeder den anderen und seine Aufgabe kennt, wenn etwas Schreckliches passiert, von den Entscheidungsträgern bis zu den Beamten auf der Straße. Vier Tage vor den London-Anschlägen haben wir damals noch eine solche Übung abgehalten. Wir haben versucht zu ergründen, wo wir am verwundbarsten wären, wenn Terroristen zuschlagen würden. Das schlimmste Szenario, das uns in den Sinn kam, waren parallele Anschläge in der U-Bahn. Natürlich konnten wir unsere Ideen bis zum 7.Juli nicht umsetzen, aber immerhin wussten wir, wo wir verwundbar sein würden."*[102]

3.6 Zusammenfassung

In diesem Kapitel wurde versucht, anhand einiger weniger eingetretener Krisen- und Katastrophenereignisse allgemeingültige Aussagen abzuleiten.

Diese lassen sich in ein paar wesentliche Kernbereiche zusammenfassen:

3.6.1 Zeitkritikalität

Komplexe und großräumige Schadenslagen sind meist sehr zeitkritisch. Für die Bewältigung bzw. Verhinderung von Eskalationen und Folgeschäden steht meist sehr wenig Zeit zur Verfügung. Diese Zeit muss vor allem durch entsprechende Krisenpräventionsmaßnahmen gewonnen werden.

3.6.2 Risiko- und Krisenkommunikation

Zur erfolgreichen Bewältigung einer Krise trägt ganz entscheidend eine entsprechende und vor allem offene und transparente Krisenkommunikation bei. Eine wesentliche Basis stellt dabei eine bereits vor der Krise durchgeführte Risikokommunikation, vor allem gegenüber der möglichen betroffenen Bevölkerung, dar.

3.6.3 Verantwortlichkeiten und Kompetenzverteilung

In fast allen Krisenlagen wird die Bewältigung durch unklare und vor allem zu stark strukturierte Verantwortungsbereiche behindert. Vor allem das föderale Prinzip stößt bei komplexen, großflächigen und vielschichtig abhängigen Schadenslagen rasch an die Grenzen der eigenen Kompetenz.

Ein Grundsatz im Krisenmanagement lautet, lieber zu früh als zu spät eskalieren. Eine Reduktion der Krisenbewältigungsorganisation ist wesentlich einfacher, als eine nachträgliche Aufstockung. Diese führt immer zu zusätzlichen Schwierigkeiten. Daher wird es erforderlich sein, die derzeitigen Krisenreaktionsfähigkeiten hinsichtlich ihrer Eignung zur Bewältigung von komplexen Schadenslagen zu überprüfen und gegebenenfalls anzupassen.

101 Vgl. Freie Universität Berlin, 2011, S. 39.

102 Vgl. „Wir wussten, wo wir verwundbar sind" URL: http://www.spiegel.de/politik/ausland/0,1518,732778,00.html [10.12.2011].

3.6.4 Krisenvorsorge und -prävention, Selbsthilfefähigkeit

Ein ganz wesentlicher Aspekt für die erfolgreiche Bewältigung, aber auch zur Vermeidung von möglichen Krisen, ist die Krisenvorsorge und -prävention. Ein besonderer Fokus ist dabei auf die Risikokommunikation und die aktive Auseinandersetzung mit möglichen Szenarien zu richten. Darüber hinaus sind entsprechende Vorkehrungen zu treffen, um im Eintrittsfall möglichst rasch und professionell reagieren zu können.

Das entscheidende Ziel der Risikokommunikation ist die Steigerung der Selbsthilfe- und Durchhaltefähigkeit jedes einzelnen Bürgers.

3.6.5 Technikfolgenabschätzung – Sicherheitsvorschriften und Kontrolle

Leider ist zu beobachten, dass immer häufiger versucht wird, neue Technologien und Vernetzungen ohne einer entsprechenden Technikfolgenabschätzung[103] und mit unzureichenden Sicherheitsmaßnahmen zu implementieren. Auf der anderen Seite sind unzureichende Sicherheitsvorschriften und vor allem auch Kontrollen festzustellen.

Dem freien Markt wird ein sehr hoher Stellenwert eingeräumt, möglicherweise ein zu Hoher. Die negativen Folgen sind in einigen Bereichen bereits deutlich spürbar. Etwa im Finanz- oder Atomenergiesektor. Gewinne werden privatisiert, Verluste sozialisiert. Banken sind zu groß, um den freien Marktgesetzen überlassen zu werden („too big to fail“).[104] Die Folgekosten von Atomkatastrophen oder für den Atommüll (Stichwort Castor-Transporte[105]) werden nicht durch die Unternehmen, sondern durch die Öffentlichkeit getragen. Diese Kosten werden auch nicht in den Strompreis hinein gerechnet, eben so wenig wie die Abwrackkosten für Atomkraftwerke. Konsequenzen, die uns in anderen Bereichen, wie etwa bei intelligenten Stromzählern, noch bevorstehen könnten.[106]

> *„Sozialisierung der Verluste und Risiken und Privatisierung der Gewinne und Vorteile. Über Resilienz zu reden und die Kehrseite nicht zu diskutieren, dass dahinter eine Bewältigungsstrategie der Folgen von Privatisierung steht, ist unredlich. Die Folge-Folge-Risiken einer solchen Strategie werden ausgeblendet, dass nämlich Völker für etwas einstehen müssen, was sie nicht wollten.“*[107]

Daher ist es um so wichtiger, dass unabhängige Organisationen geschaffen werden, die in der Lage sind, technische Details zu erfassen und in einen Gesamtzusammenhang zu bringen. Besonders durch die immer weiter fortschreitende Vernetzung entstehen bisher kaum bekannte Risiken. Vernetzung bringt nicht nur Vorteile, sondern schafft zusätzlich ganz neue Abhängig- und Verwundbarkeiten. Daher sind neben den unabhängigen Technikfolgenabschätzungen ebenso entsprechende Sicherheitsvorschriften mit qualifizierten Kontrollen und Konsequenzen unabdingbar. Nur so können

103 Duden: „interdisziplinäre Forschungsrichtung, die Chancen und Risiken sowie die gesellschaftlichen Folgen technischer Neuerungen untersucht“.

104 Vgl. „28 Banken sind "too big to fail"“ http://www.zeit.de/wirtschaft/unternehmen/2011-07/Banken-Commerzbank-Draghi [30.12.2011].

105 Vgl. „Castor-Transport nach Gorleben verursacht Rekordkosten“ URL: http://www.haz.de/Nachrichten/Politik/Niedersachsen/Castor-Transport-nach-Gorleben-verursacht-Rekordkosten [30.12.2011].

106 Vgl. „Die dunkle Seite der Spitzentechnologie“ URL: http://www.sueddeutsche.de/wissen/2.220/riskante-forschung-die-dunkle-seite-der-spitzentechnologie-1.1112690 [08.12.2011].

107 Freie Universität Berlin, 2011, S. 39.

die tatsächlichen Restrisiken klein und die Folgen für die Gesellschaft beherrschbar gehalten werden. Das Krisenmanagement beruht vor allem auf dem Handeln vor der Krise!

„Those who cannot remember the past are condemned to repeat it."
George Santayana

4 Stromversorgungssicherheit

Strom ist die wichtigste Lebensader einer modernen Gesellschaft, da so gut wie alle anderen Lebensadern – die strategischen Infrastrukturen – von der Verfügbarkeit von Strom abhängen (siehe Abbildung 5). Weite Teile der lebenswichtigen, strategischen Infrastruktur aber auch unser gesamtes Gemeinwesen funktionieren nur durch eine verlässliche Energieversorgung, daher wurde viel Wert auf die Verfügbarkeit von elektrischer Energie gelegt. Künftig muss aber noch mehr Wert darauf gelegt werden, um großflächige und längerfristige Stromausfälle und deren kurz-, mittel- und langfristig katastrophalen Schäden für die gesamte Gesellschaft zu verhindern bzw. eine professionelle Schadensbegrenzung durchführen zu können.[108]

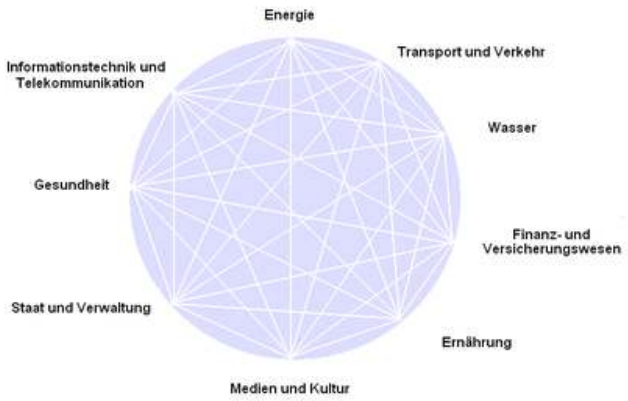

Abbildung 5: Inderdependenzen - Quelle: http://www.kritis.bund.de

An zweitwichtigster Stelle folgen die Informations- und Kommunikationstechnikinfrastrukturen. Ohne technische Kommunikation sind viele Lebensbereiche nur mehr sehr eingeschränkt funktionsfähig. Diese sind aber wiederum ganz wesentlich von der Verfügbarkeit von Strom abhängig.

Bisher gab es in Europa kaum schwerwiegende, großräumige Stromausfälle. Durch die umfassende Vernetzung und Computerisierung haben sich aber in den vergangenen Jahren völlig neue Abhängigkeiten ergeben, die nur mehr sehr schwer zu durchschauen sind. Damit steigt die Fehleranfälligkeit, die Widerstandsfähigkeit („Resilience“) der hochkomplexen Systeme, auf denen unser Gemeinwesens basiert, sinkt. Unsere Gesellschaft ist daher gut beraten, sich intensiver mit diesen Risiken auseinanderzusetzen, denn eines der folgenschwersten Ereignisse für unsere hoch technisierte Zivilisation ist ein großräumiger, länger andauernder Stromausfall, ein Blackout.

4.1 Blackout

Hinter dem englischen Begriff verbirgt sich die etwas sperrige Beschreibung für einen plötzlichen, großräumigen und länger andauernden Stromausfall, wobei es keine klare quantitative Eingrenzung gibt. In dieser Arbeit wird mit dem Begriff Blackout ein Stromausfall in einem großflächigen Gebiet assoziiert, wobei nicht einfach externe Hilfe zugeführt werden kann, bzw. dessen Dauer länger als eine Stunde beträgt.

Die Auswertung von bisherigen Blackouts hat ergeben, dass diese in der Regel von ein bis zwei nicht verbundenen Ereignissen ausgelöst wurden, die dominoartig zu Abschaltungen von Kraftwerken, Übertragungsleitungen und Schaltanlagen führten. Vor allem extreme Wetterbedingungen, menschliches Versagen und technische Mängel, oder eine Kombination dieser Faktoren, waren die häufigsten Ursachen.[109]

108 Vgl. CRO Forum, 2011, S. 4.
109 Vgl. Zeitung für kommunale Wirtschaft, 2003, S. 1.

Europa ist bisher weitgehend von großen Blackouts verschont geblieben bzw. sind die Ereignisse von 2003 oder 2006 bereits wieder in Vergessenheit geraten. Schwerwiegende Zwischenfälle sind vor allem aus den USA bekannt, wo es immer wieder infolge von Naturereignissen oder durch technische Mängel, die etwa auf die Privatisierung der Strominfrastruktur zurückzuführen sind, zu Blackouts kommt. Das amerikanische Stromnetz gehört überhaupt zu den anfälligsten aller Industriestaaten. Hier werden Schäden durch Blackouts in der Höhe von 150 Milliarden Dollar pro Jahr kolportiert.[110] [111]

Das zentraleuropäische Stromnetz zählt bisher weltweit zu den stabilsten. Dass das nicht unbedingt linear in die Zukunft projiziert werden kann, muss aufgezeigt werden. Das deutsche Zukunftsforum öffentliche Sicherheit stellte dazu bereits 2008 in seinem Grünbuch fest:

> *„Die mittelbare und unmittelbare Eintrittswahrscheinlichkeit ist hoch. Auch besteht ein hohes Risiko für Menschen, Staat und Wirtschaft. Denn ein Stromausfall würde große Schäden verursachen, unter anderem Sachschäden durch unmittelbare Zerstörung und Folgeschäden wie Versorgungsausfälle und Lieferunterbrechungen."*[112]

Daher ist es wichtig, die Bürger zu sensibilisieren und zur Übernahme von Eigenverantwortung zu animieren. Dies betrifft vor allem die Vorsorge im eigenen Umfeld, welche mit der einfachen Auseinandersetzung mit den möglichen Szenarien beginnt und bis hin zu einer Eigenbevorratung und persönlichen Notfallplanung führt. Wer emotional betroffen ist, wird auch darauf achten, wie Verantwortungs- und Entscheidungsträger mit dieser Thematik umgehen. Nur so kann es gelingen, diesem Thema neben den unzähligen anderen Themen an entsprechender Stelle Gehör zu verschaffen. Die möglichen Konsequenzen einer nicht verfügbaren Stromversorgung sind zu schwerwiegend, als dass bis zu einem möglichen Eintritt zugewartet werden kann. Bei der bisherigen Bearbeitung dieses Themas wurde immer wieder Unverständnis festgestellt. In den seltensten Fällen ist die volle Tragweite eines Blackouts bewusst.

In diesem Zusammenhang erscheint ein Zitat von Professor Walter Seledec

> *„Anfang August erreichten uns Alarmmeldungen von den Britischen Inseln, die man kaum glauben konnte oder besser, deren Inhalt unserer bisherigen Vorstellung widersprach."*[113]

angebracht. Nur weil derzeit etwas nicht unseren Vorstellungen entspricht, bedeutet das leider noch lange nicht, dass es nicht dennoch eintreten kann. Es werden daher hier einige Aspekte beleuchtet, welche die Eintrittswahrscheinlichkeit eines derartigen Ereignisses hoffentlich in einem anderen Licht erscheinen lassen werden. Einstellungen wie „Das wird schon nicht so schlimm werden!" oder „Das haben wir alles im Griff!" sind im höchsten Maße unverantwortlich.

110 Vgl. „Warum die USA den Blackout in Kauf nehmen" URL: http://independence.wirsol.de/news/warum-die-usa-den-blackout-in-kauf-nehmen/4133 [08.12.2011].

111 Vgl. CRO Forum, 2011, S. 16.

112 Zukunftsforum öffentliche Sicherheit, 2008, S. 19.

113 Die Lehren aus London, TRUPPENDIENST, Heft 5/2011, Seite 430, vgl. URL: http://www.bundesheer.at/truppendienst/ausgaben/artikel.php?id=1190 [04.12.2011].

Bereits nach etwa 24 Stunden Stromausfall muss mit einer besonders kritischen Lageentwicklung gerechnet werden. Durch die fehlende Notstromversorgung von Tankstellen und Tanklagern ist ein völliges Zusammenbrechen der Mobilität und der Kommunikationsmöglichkeiten, auch für Einsatzorganisationen, zu erwarten.[114]

Das ein Totalausfall möglicherweise nicht in wenigen Stunden zu beheben ist wird sogar durch den Technikvorstand der Austrian Power Grid (APG) in einem Presseinterview eingestanden:

> *„Es ist allerdings unwahrscheinlich, dass ein Blackout nach 24 Stunden vorbei ist. 'Das Hochfahren nach einem Totalausfall kann bis zu einer Woche dauern', sagt Heinz Kaupa, Technikvorstand der Austrian Power Grid (AGP), die in Österreich 95 Prozent des Übertragungsnetzes betreibt. Auch die Wahrscheinlichkeit dafür steigt. 2003 und 2006 registrierte man in der Schweiz und in Deutschland Zwischenfälle, die nur um Haaresbreite keinen Blackout auslösten. Kaupa: 'Damals hatten wir richtig Glück.' Generell beobachtete die APG in den vergangenen Monaten, dass die Netze immer labiler werden."*[115]

Eine aktuelle Analyse des deutschen Büros für Technikfolgenabschätzung hält darüber hinaus über die weitere Lageentwicklung fest:

> *„Spätestens am Ende der ersten Woche wäre eine Katastrophe zu erwarten, d. h. die gesundheitliche Schädigung bzw. der Tod sehr vieler Menschen sowie eine mit lokal bzw. regional verfügbaren Mitteln und personellen Kapazitäten nicht mehr zu bewältigende Problemlage."*[116]

Diese Analyse enthält auch sonst sehr tief gehende Betrachtungen und Denkanstöße und ist daher auch für Österreich als wichtiges Basismaterial zu klassifizieren.

Es muss daher bereits jetzt festgelegt werden, welche zusätzlichen organisatorischen Maßnahmen zu den bisher getroffenen Krisen- und Katastrophenschutzvorkehrungen notwendig sind, um solchen Zusammenbruchsszenarien gesamtgesellschaftlich bestmöglich begegnen zu können. Hier sollen Denkanstöße und nicht fertige Lösungen geliefert werden. Die Thematik ist zu komplex, als dass sie von Einzelpersonen und losgelöst von verschiedenen vorhandenen Strukturen und Organisationen endgültig betrachtet werden könnte.

Um das Szenario gesamtheitlich zu erfassen, wird es in weiterer Folge auch notwendig sein, mögliche Angriffe auf die Stromversorgung im Rahmen von Cyber-Konflikten zu betrachten. Einen ersten Vorgeschmack auf diese Problematik hat die technisierte Welt mit der 2010 bekannt gewordenen Schadsoftware STUXNET[117] bekommen. Nach kaum verifizierbaren Informationen dürfte diese Schadsoftware gegen ein ganz spezielles und gut geschütztes Ziel, das iranische Atomprogramm bzw. die dafür erforderlichen

114 Vgl. Ladinig, 2010.

115 Vgl. „Blackout: Was, wenn der Strom ausbleibt?" URL: http://diepresse.com/home/panorama/oesterreich/701402/Blackout_Was-wenn-der-Strom-ausbleibt [09.01.2012].

116 Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 10.

117 STUXNET Ein Cyber War Angriffsprogramm?, TRUPPENDIENST, Heft 2/2011, Seite 148ff, vgl. URL: http://www.bundesheer.at/truppendienst/ausgaben/artikel.php?id=1119 [04.12.2011].

Urananreicherung, gerichtet gewesen sein.[118] Diverse Quellen sprechen von einem erfolgreichen Angriff. Um wie viel einfacher könnte ein solcher Angriff auf die viel weniger geschützte und aufgrund der vielen Schnittstellen auch nicht wirklich vollständig zu sichernde Strominfrastruktur sein? In dieser Arbeit werden diese Szenarien jedoch nicht weiter betrachtet. Eine gute Krisenprävention im Bereich der Stromversorgung wird aber ebenso einen Beitrag zum Schutz vor derartigen Szenarien liefern.

Das Österreichische Bundesheer wird bei einem großen Blackout eine sehr wichtige Rolle einnehmen müssen. Daher sind bereits jetzt entsprechende Ableitungen und Vorbereitungsmaßnahmen in enger Kooperation mit den Blaulichtorganisationen und Energieversorgungsunternehmen (EVU) zu treffen. Es muss davon ausgegangen werden, dass die technischen Kommunikationsmöglichkeiten im Anlassfall weitgehend ausfallen werden. Entsprechende Planspiele und Übungen sind daher für eine erfolgreiche Krisenreaktion ganz essentiell. Nur so können die entsprechenden Lehren vorzeitig gezogen, Verbesserungsmaßnahmen umgesetzt und im Anlassfall vorbereitete und automatisierte Abläufe mit geringem Kommunikationsaufwand aktiviert werden.

Durch eine österreichische Forschungseinrichtung wurde im Rahmen des KIRAS[119] Projekts *BlackÖ.I*[120] aufbauend auf bereits vorhandene Grundlagen und Erkenntnisse ein umfangreiches Berechnungsmodell über den wahrscheinlichen volkswirtschaftlichen Schaden durch ein Blackout in Österreich erstellt, in welchem sehr viele Parameter berücksichtigt werden. Das Projekt kommt zum Schluss, dass je nach Jahres- und Tageszeit enorme finanzielle Verluste zu erwarten sind. So ist etwa bei einem österreichweiten, einstündigen Blackout an einem Novembertag beginnend um 9 Uhr Vormittag mit einem Gesamtschaden von rund 180 Millionen Euro zu rechnen. Dauert das selbe Blackout 24 Stunden, so sind Kosten von etwa 890 Millionen Euro zu erwarten. Summen, die wohl so manche Vorstellungskraft sprengen. Die endgültige Freigabe des Gesamtberichtes ist für Ende des ersten Quartals 2012 beabsichtigt.

4.1.1 Ursachen für ein Blackout

Die Ursachen für einen lang andauernden und überregionalen Stromausfall können vielfältig sein[121] [122]:

- Menschliches Versagen (Schaltfehler, Fehlreaktionen, Unaufmerksamkeit, etc.);
- Systemische, organisatorische Mängel (Netzaufsplitterung, fehlende Übertragungsleitungen, deutlich unausgeglichenes Angebot- und Nachfrageverhalten, übertriebenes Gewinnstreben, mangelhafte oder fehlende Instandhaltung, etc.);
- Ressourcen/Ausfall der Primärenergie (mangelnde Kühlfähigkeiten für Kraftwerke, Mangel an Wasser, Wind, Öl, Gas, Kohle oder Brennstäben, etc.);

118 Vgl. „Der Stuxnet-Wurm“ URL: http://www.symantec.com/de/de/business/theme.jsp?themeid=stuxnet [04.12.2011].

119 Österreichische Förderungsprogramm für Sicherheitsforschung; vgl. URL: http://www.kiras.at/ [04.12.2011].

120 Blackouts in Österreich Teil I – Analyse der Schadenskosten, Betroffenenstruktur und Wahrscheinlichkeiten großflächiger Stromausfälle.

121 Vgl. URL: www.noezsv.at/noe/media/0_Dokumente/KKM_blackout.pdf [29.05.2011].

122 Vgl. CRO Forum, 2011, S. 9.

- Technisches Versagen (Wartungsmängel, Überalterung von Anlagen, Fehldimensionierungen von Betriebsmitteln, mangelhafte Planung & Umsetzung, Materialfehler, Produktionsfehler, Ausfall von zentralen Betriebsmitteln, etc.);
- Klima/Klimawandel/Naturereignisse (Hitze/ Kältewellen, Blitzschlag, Stürme, Hochwasser, Schnee/Eis, Erdbeben, Sonnenstürme, etc.);
- Pandemie (krankheitsbedingter Ausfall von Betriebspersonal);
- Kriminalität/Terrorismus (Diebstahl, Betrug, Erpressung, Sabotage, Anschläge, Kabeldiebstahl, Cyber Angriff auf Steuersysteme, etc.);
- Kriegerische Auseinandersetzungen (Zerstörung von elektronischen Bauteilen durch einen elektromagnetischen Puls /EMP, Einsatz von Cyber Waffen).

In weiterer Folge werden einige mögliche Ursachen näher beschrieben, die jederzeit unter Berücksichtigung des (n-1)-Kriteriums[123] zu einem Blackout führen können bzw. die Basis dazu liefern. Dabei werden nur Ursachen berücksichtigt, die derzeit permanent anzutreffen sind. Menschliche Ursachen, wie Sabotage oder gezielte Angriffe, werden in dieser Arbeit nicht behandelt.

4.1.2 Unmittelbare Folgen eines Blackouts

Ein Zusammenbruch der Stromversorgung wirkt sich ohne Vorwarnung und übergangslos zu 100 Prozent auf alle elektrischen Geräte und Einrichtungen aus. Ausgenommen sind solche Stromverbraucher, die durch Batterien oder Akkus ersatzweise durch eine temporäre unterbrechungsfreie Stromversorgung (USV)[124] versorgt werden. Ebenfalls nicht unmittelbar betroffen sind jene Verbraucher, die für diesen Notfall an eine Netzersatzanlage, etwa in Form eines Notstromaggregates, angeschlossen sind.[125] In unserer heutigen Welt bedeutet das, dass die Grundversorgung weitgehend zusammenbricht.[126]

Für den Einzelnen sind die Folgen sehr vielschichtig. Unmittelbar ist die Beleuchtung, weitgehend die technische Kommunikation (Telefonie, Internet, Mobiltelefonie), Rundfunk, Heizung, Kühlung, zum Teil die Wasser Ver- und Entsorgung, die Treibstoffversorgung sowie der (Finanz-)Handel betroffen.

Im Bereich der Telekommunikation fallen sofort oder nach kurzer Zeit große Bereiche der Infrastruktur aus. Davon betroffen sind vor allem digitale Festnetztelefone und analoge Schnurlostelefone. Das Mobilfunknetz bleibt mit Teilen noch temporär verfügbar, wird aber wahrscheinlich noch mehr sehr eingeschränkt nutzbar sein. Größere Basisstationen sind über einen kurzen Zeitraum notstromversorgt. Die Sprachkommunikation wird durch Überlastung sehr rasch zusammenbrechen. Die Verwendung von SMS könnte noch am längsten funktionieren. Vor allem im urbanen Bereich, mit nicht notstromversorgten, vorwiegend Mikrozellen, ist ein weitgehender sofortiger Zusammenbruch zu erwarten. Die klassische, analoge Telefonie wird wahrscheinlich noch am längsten zur Verfügung stehen. Jedoch steigen immer mehr Haushalte und Orga-

123 siehe Abschnitt 4.2.1 (n-1)-Kriterium

124 Diese dient in der Regel dazu, kurzfristige Stromversorgungsunterbrechungen zu überbrücken, bzw. ein ordnungsgemäßes Herunterfahren von Systemen, z. B. von Servern, zu ermöglichen, um Schäden an der Hardware bzw. an den Daten zu verhindern. Eine USV dient nicht zur Aufrechterhaltung des Betriebes!

125 Vgl. CRO Forum, 2011, S. 4.

126 Eine umfassendere Beschreibung der Lageentwicklung steht beim Verfasser zur Verfügung und wird auch in der Zeitschrift TRUPPENDIENST, im Heft 2/2012, erscheinen.

nisationen auf digitale Telefonie und Telefonanlagen um und sind somit sofort betroffen. Ob die Übertragungswege weiterhin funktionieren, wird sich erst im Anlassfall zeigen.[127] [128]

> *„Die Vielzahl der strombetriebenen Netzwerkknoten, Vermittlungsstellen und Funkantennen der Festnetz- und Mobiltelefonie sowie des Internets macht deren flächendeckende Wiederinbetriebnahme praktisch unmöglich, da Tausende von Batteriespeichern geladen und Treibstofftanks versorgt werden müssten. Allenfalls an den Rändern des vom Stromausfall betroffenen Gebiets ist eine teilweise Reaktivierung einzelner Infrastrukturelemente denkbar."*[129]

Bereits unmittelbar nach einem Blackout ist – durch eine gesteigerte Anzahl von medizinischen und unfallbedingten Notfällen – mit einem deutlichen Anstieg von Verletzten und auch Todesopfern zu rechnen. Einerseits, da Rettungskräfte nicht zum Notfallort gerufen werden können bzw. diese aufgrund eines Verkehrschaos den Notfallort nicht rechtzeitig erreichen, andererseits da aufgrund der Häufung von Notfällen nicht ausreichend Einsatzkräfte zur Verfügung stehen. [130]

Blackouts im Winter erhöhen die Gefahrenlage deutlich. Nicht nur elektrische Heizsysteme benötigen Strom, auch andere Heizsysteme, wie etwa Gasthermen, erfordern für den Betrieb eine funktionierende Stromversorgung. Darüber hinaus müssen verstärkt Brände durch unsachgemäße Feuerstellen erwartet werden. Bei gleichzeitigem Wassermangel könnte das katastrophale Auswirkungen nach sich ziehen.[131]

Besonders schwerwiegende Folgen sind in urbanen Räumen zu erwarten. Auch hier wird es sehr vielschichtige Folgen geben. Die größte Herausforderung dürfte dabei die Rettung von in Aufzügen oder auch in U-Bahnen eingeschlossenen Personen darstellen. Insbesondere, da in größeren Ballungsräumen sehr rasch ein Verkehrskollaps zu erwarten ist.

Ein besonders kritischer Bereich könnte auch die (Abwasser)Entsorgung darstellen, wenn nicht entsprechende Vorkehrungen getroffen wurden. Wahrscheinlich vielfach nicht besonders beachtet, sollte aber der Strombedarf z. B. der Hauptkläranlage Wien zum Nachdenken anregen. Diese verbraucht rund 1 % des gesamten Strombedarfs der Stadt Wien. „Derzeit werden für die Reinigung des gesamten Wiener Abwassers jährlich 60 GWh Strom benötigt (= Verbrauch von rund 20.000 Haushalten)."[132] Je nach Dauer muss bei einem Ausfall der Entsorgung oder von Teilbereichen (-prozessen) eine folgenschwere Eskalation erwartet werden. Es kann etwa erforderlich werden, dass Hochhäuser aufgrund einer fehlenden Wasser Ver- bzw. insbesondere Entsorgung, evakuiert werden müssen. Eine nicht funktionierende Entsorgung könnte vor allem in der warmen Jahreszeit sehr rasch zu einem Hygieneproblem und damit zu ei-

127 Vgl. Zukunftsforum öffentliche Sicherheit, 2008, S. 23.
128 Vgl. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 30ff.
129 ebenda, S. 5.
130 Vgl. ebenda, S. 79.
131 Vgl. CRO Forum, 2011, S. 12.
132 Vgl. „Kooperation Wien Energie und Hauptkläranlage Wien" URL: http://www.wienerstadtwerke.at/eportal/ep/contentView.do/contentTypeId/1001/channelId/-30566/programId/13111/pageTypeId/11083/contentId/27784 [16.12.2011].

ner Seuchengefahr führen, da z. B. die Notdurft nur mehr bedingt ordnungsgemäß verrichtet werden kann.[133]

Eine unvorbereitete Bevölkerung wird daher umso schlimmer von einem Blackout getroffen. Durch mangelnde Informations- und Kommunikationsmöglichkeiten muss damit gerechnet werden, dass die Lage teilweise eskaliert. Ein wesentlicher Faktor ist dabei das soziale Gefüge vor dem Ereignis. Im ländlichen Raum wird dies eher zum Zusammenhalt und zur Nachbarschaftshilfe führen. Kritischere Entwicklungen müssen vor allem in urbanen Räumen erwartet werden, insbesondere dann, wenn die Versorgung mit Grundnahrungsmittel nicht mehr aufrechterhalten werden kann.[134] [135]

Viele kritische Infrastrukturbereiche, wie etwa Krankenhäuser, Einsatzzentralen von Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Kommunikationsknoten und Steuerzentralen sind mit Netzersatzanlagen ausgestattet. Die netzunabhängige Betriebsdauer hängt wesentlich vom vor Ort gelagerten Treibstoff ab, da davon ausgegangen werden muss, dass die Anschlussversorgung nicht funktionieren wird.[136] Einerseits, da die Kommunikation zum Versorgungsunternehmen nur eingeschränkt möglich sein wird und andererseits eine Notstromversorgung im Bereich der Treibstoffversorgung die Ausnahme darstellt bzw. im Zuge vom anzunehmenden Verkehrschaos ein Fortkommen nur eingeschränkt möglich sein wird.

Sofort und unmittelbar betroffen sind auch sämtliche Logistikbereiche, die ganz wesentlich für die Grundversorgung der Bevölkerung relevant sind. Das heutige Modell der „Just-in-time“ Logistik wird sich daher besonders rasch und nachteilig negativ auswirken.

> *„Sollte die Bevölkerung keine ausreichende Unterstützung von behördlicher Seite erhalten, wird sie sich eigene Wege für ihre Versorgung suchen. Diese werden nicht zwingend rechtsstaatlichen Grundsätzen genügen.“*[137]

Besonders kritisch könnte die Lage in der Produktion werden und dies innerhalb sehr kurzer Zeitspannen. So entstehen z. B. in der Aluminiumindustrie bereits nach 4-5 Stunden Stromausfall irreversible Schäden an der Produktionsanlage.[138] Ähnliche Situationen sind auch in der Lebensmittelindustrie zu erwarten, wo beispielhaft Schokolade in den Transportleitungen aushärtet und die Produktionsanlagen zerstört.

Derzeit gibt es keine klaren Handlungsanweisungen bzw. Notfallpläne für Betreuungseinrichtungen, insbesondere für Kindergärten und Schulen, wie bei einem Blackout zu verfahren ist. Die Pädagoginnen und pädagogischen Hilfskräfte haben oft eigenen Nachwuchs, der wohl zum Großteil in anderen Bildungseinrichtungen betreut wird. Mangels Kommunikationsmöglichkeiten werden diese nach relativ kurzer Zeit versuchen, zu ihren eigenen Kindern zu gelangen. Damit könnte die Lage für die Zurückgebliebenen relativ rasch eskalieren. Je nach Jahreszeit werden wahrscheinlich zusätzliche kritische Faktoren eine Rolle spielen, etwa im Winter (kein/kaum Licht, die Hei-

133 Vgl. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 7.
134 Vgl. Zukunftsforum öffentliche Sicherheit, 2008, S. 23.
135 Vgl. Forschungsforum Öffentliche Sicherheit, 2010b, S. 3f.
136 Vgl. CRO Forum, 2011, S. 12.
137 Vgl. Zukunftsforum öffentliche Sicherheit, 2008, S. 23.
138 Vgl. CRO Forum, 2011, S. 12.

zung fällt aus, Essen kann nicht gewärmt werden, usw.). Auch die Eltern wissen nicht, was in den Bildungseinrichtungen passiert und werden daher zusätzlich verunsichert und danach trachten, möglichst rasch ihre Kinder in Sicherheit zu bringen, was das Chaos zusätzlich verstärken wird.[139]

Die Beispiele könnten unendlich fortgesetzt werden und übersteigen wohl fast jede Vorstellungskraft.

Je nach Jahres- und Tageszeit werden sich die Folgen entsprechend rasch auswirken. Die großen Blackouts von 2003 und 2006 ereigneten sich außerhalb der Aktivzeit der meisten Menschen, in den Abend- und Nachtstunden und sie wurden großteils in dieser Zeit noch behoben. Daher waren die Folgen beschränkt bzw. wurde der Zwischenfall vom Großteil der Bevölkerung wahrscheinlich kaum wahrgenommen. Ereignet sich ein solcher Zwischenfall während der Tageszeit oder dauert dieser länger an, dann ist mit völlig anderen Konsequenzen zu rechnen.

4.1.3 Blackout 2003 – Italien

Italien kann seinen Strombedarf nicht selbst decken und muss einen wesentlichen Teil des Eigenbedarfs aus der Schweiz bzw. aus Frankreich beziehen.

Am 28.August 2003 begann in Graubünden/Schweiz eine Verkettung von Ereignissen, die binnen einer halben Stunde in ganz Italien zu einem Blackout führten. In den frühen Morgenstunden schloss eine wichtige Freileitung („Stromtransitleitung“) durch einen Baum kurz. Diese wurde daraufhin automatisch abgeschaltet. Mehrfache Versuche, die unterbrochene Verbindung wieder in Betrieb zu nehmen, scheiterten. Daher musste eine benachbarte Leitung eine höhere Leistung aufnehmen. Kurz darauf führte die Mehrbelastung dieser Leitung zur erhöhten Erwärmung und zum starken Durchhängen, was wiederum zu einem Kurzschluss durch einen Baum führte. Nach dem Ausfall der beiden wichtigen Freileitungen folgte innerhalb von zwölf Sekunden kaskadenartig die Abschaltung der anderen grenzüberschreitenden Stromtransportleitungen nach Italien. In dieser Phase der Instabilität kam es in Norditalien zu einer starken Netzinstabilität, welche die Notabschaltung mehrerer Kraftwerke zum Eigenschutz bewirkte. Das italienische Stromversorgungssystem war nicht mehr in der Lage, die nunmehr vom Ausland abgeschnittene Stromversorgung, im Inselbetrieb, aufrechtzuerhalten oder kontrollierte Abschaltungen durchzuführen. Zweieinhalb Minuten nach der Trennung vom übrigen Netz kollabierte in ganz Italien die Stromversorgung.

Mehr als 110 Züge mit rund 30.000 Passagieren waren in weiterer Folge stundenlang während der Nacht blockiert. Tausende saßen in Bahnhöfen und in Flughäfen fest. In dem Chaos, das rund 56 Millionen Bürger betraf und in einzelnen Regionen bis zu 18 Stunden dauerte, kamen zumindest fünf Menschen durch Unfälle ums Leben.[140] [141] [142]

139 Diese Ableitungen können aufgrund unmittelbarer eigener Betroffenheit und Rücksprachen mit der MA10 (Kindergärten in Wien) getroffen werden.

140 Vgl. „Stundenlanger Stromausfall in ganz Italien“ URL: http://www.udo-leuschner.de/energie-chronik/030901.htm [31.10.2011].

141 Vgl. Energietechnische Gesellschaft im VDE, 2003.

142 Vgl. CRO Forum, 2011, S. 27.

4.1.4 Blackout 2005 – Deutschland

Im November 2005 bildeten sich infolge von mehreren Extremwetterereignissen schwere Schnee- und Eislasten auf den Stromleitungen, starke Winde und zusätzlicher Regen begünstigten einen Zusammenbruch der rund 50 Jahre alten Strommasten. Dies führte zum Ausfall von 5 Freilandleitungen.

> *„Als Ursache für das Versagen des Mastens 65 in BL1503 konnte die Kombination aus wetterbedingt hohen einseitigen Zusatzlasten und Bauteilen aus verspröde-tem Thomasstahl widerspruchsfrei identifiziert werden."*[143]

Der mehrtägige Stromausfall im dünn besiedelten Münsterland löste Schäden von schätzungsweise 130 Millionen Euro aus.[144]

Ein späterer Untersuchungsbericht hält dabei fest:

> *„Zu der Schadenssituation im Münsterland ist es nur gekommen, weil mehrere Schadensauslöser gleichzeitig aufgetreten sind."*[145] *(…) „Eine Erkenntnis aus den Ursachen der Versorgungsstörung im November 2005 ist, dass ein solcher Störfall sich überall erneut ereignen kann."*[146]

Eine besondere Erfahrung war auch, dass „die Stäbe auf Kreisebene zum Teil personell nicht in der Lage waren, einen 24-Stunden-Betrieb im Verwaltungs- und Einsatzstab aufrechtzuerhalten."[147]

Ein weiteres Problem stellte die fehlende Übersicht über die verfügbaren Ressourcen dar. Insgesamt waren rund 300 Notstromaggregate unterschiedlichster Leistungsstärke und aus dem gesamten Bundesgebiet, sowie rund 4.000 Helfer eingesetzt.[148]

4.1.5 Blackout 2006 – Süd-Westeuropa

Eine andere, ebenfalls kaum zu verhindernde Ursache, nämlich menschliches Versagen, führte am 4.November 2006 kurz nach 22 Uhr zu einem Blackout, dass einen noch weit größeren geografischen Raum umfasste. Durch mangelhafte Planung, kurzfristige Änderungen und Kommunikationsfehler beim Bedienungspersonal, kam es bei der geplanten Abschaltung einer Hochspannungsleitung im Raum Hamburg zu einer Kettenreaktion. Teile von Deutschland, Frankreich, Belgien, Italien, Österreich und Spanien waren bis zu 120 Minuten ohne Strom. Betroffen waren mehr als 15 Millionen Haushalte.[149] [150]Durch das rasche Handeln des operativen Personals konnte ein österreichweites Blackout gerade noch verhindert werden. Aufgrund des noch nicht Fertiggestellten 380 kV-Ringes[151] lief die europaweite Trennungslinie quer durch Ös-

143 Bundesamt für Materialforschungund prüfung: *Schadensanalyse an im Münsterland umgebrochenen Strommasten.* In: Internet, 2006, unter URL: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Energie/Sonderthemen/VersorgungsstoerungMuensterland05/BAMGutachtenId6409pdf.pdf?__blob=publicationFile [12.12.2011], S. 2.

144 Zukunftsforum öffentliche Sicherheit, 2008, S. 19.

145 Vgl. Bundesnetzagentur, 2006, S. 5.

146 Vgl. ebenda, S. 6.

147 Zukunftsforum öffentliche Sicherheit, 2008, S. 23.

148 ebenda, S. 25.

149 Vgl. Bundesnetzagentur, 2007.

150 Vgl. CRO Forum, 2011, S. 28.

151 Vgl. Abschnitt 4.3.2, Das österreichische Stromnetz.

terreich. Durch diesen fehlenden Lückenschluss stellt das österreichische Hochspannungsnetz nach wie vor eine Schwachstelle im europäischen Verbundnetz dar.[152] Aufgrund der Tageszeit (22 Uhr) blieb das Blackout wohl weitgehend unbemerkt bzw. ohne schwerwiegende Folgen.

Diese Beispiele zeigen sehr deutlich, wie ein grundsätzlich relativ unbedeutendes Ereignis binnen weniger Minuten von einer friedlichen Lage zum Ausnahmezustand für Millionen von Menschen führen kann. In beiden Fällen war es wohl Glück, dass das Blackout nicht in der aktiven Arbeitszeit eintrat und daher nur beschränkt Folgen zu verzeichnen waren.

4.1.6 Verletzlichkeitsparadoxon

Das „Verletzlichkeitsparadoxon" beschreibt den Widerspruch zwischen Risikowahrnehmung und Realität. Die meisten technisch entwickelten Nationen weisen eine relativ zuverlässige, über lange Zeiträume funktionierende Stromversorgung auf.[153] Darüber hinaus bauen nahezu alle technischen Systeme und sozialen Handlungen auf dieser relativen Verlässlichkeit auf. Nicht oder nur unzureichend wird die damit einhergehende massive Verletzbarkeit berücksichtigt. Darüber hinaus führt dies dazu, dass oft aus Kostendruck, Versorgungsleistungen zunehmend weniger störsicher errichtet und betrieben werden.[154] [155]

Ein mögliches Blackout trifft daher eine unvorbereitete Gesellschaft umso härter.

4.2 Technische Faktoren

In diesem Abschnitt werden Faktoren beschrieben, die für ein Blackout relevant sein können und vor allem dem technischen Bereich zuzuordnen sind.

4.2.1 (n-1)-Kriterium

Überregionale Stromnetze werden nach dem (n-1)-Kriterium betrieben. Das bedeutet, dass die automatischen Regel- und Sicherheitseinrichtungen so konfiguriert sind, dass zu jeder Zeit ein elektrisches Betriebsmittel, etwa Teile eines Umspannwerkes, eine Hochspannungsleitung oder ein Kraftwerk ausfallen darf, ohne dass es zu einer Überlastung eines anderen Betriebsmittels oder gar zu einer Unterbrechung der Energieversorgung kommt. Wenn beispielsweise eine Überlandleitung aus irgendeinem Grund ausfällt, wird automatisch und unterbrechungsfrei der Strom auf andere Leitungen verteilt und die schadhafte Stelle wird umgangen. Tritt aber zeitgleich ein weiterer Fehler im benachbarten Segment auf, kommt es zu einer Überbelastung des regionalen Netzes und die betroffenen Betriebsmittel werden zum Eigenschutz automatisch abgeschaltet. Im korrekt betriebenen System müssen also mindestens zwei Ereignisse zusammentreffen, damit überhaupt eine Versorgungsunterbrechung entstehen kann. Dies kann dann zu einem Dominoeffekt und zu großräumigen Abschaltungen führen, welche in einem Blackout enden.[156]

152 Vgl. „Blackout gerade noch verhindert" URL: http://www.waltner.co.at/stromausfall.html [31.10.2011].
153 Vgl. „Österreich: Versorgungssicherheit gewährleisten" URL: http://oesterreichsenergie.at/die-versorgungssicherheit-in-oesterreich-ist-gewaehrleistet.html [22.11.2011].
154 Vgl. Forschungsforum Öffentliche Sicherheit, 2010a, S. 17.
155 Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 17.
156 Vgl. Bundesnetzagentur, 2007, S. 17.

Bei Ausfall eines Betriebsmittels ist es die Aufgabe des Netzwerkmanagements, durch entsprechende Steuerungsmaßnahmen, das (n-1)-Kriterium möglichst rasch wieder herzustellen. Im Bereich der Hochspannungsebene funktionieren diese Maßnahmen in der Regel unterbrechungsfrei und automatisch, auf der Mittelspannungsebene geht es im Regelfall nicht ohne Unterbrechung.

4.2.2 70 Prozent-Regel

Eine wichtige Voraussetzung für den sicheren Netzbetrieb nach dem (n-1)-Kriterium ist die „70 Prozent-Regel". Dies bedeutet, dass Hochspannungsleitungen nur mit 70 Prozent der vorgesehenen Gesamtbelastbarkeit auf Dauer betrieben werden sollen, um bei Bedarf entsprechende Reserve- bzw. Überkapazitäten aufnehmen zu können.[157] Wenn diese Reserve nicht ausreicht oder durch eine bereits erhöhte Grundlast ausgeschöpft ist, kann dies zu einer folgenschweren Sicherheitsabschaltung, wie 2003 in der Schweiz, führen.[158]

4.2.3 50,2 Hertz Problem

Photovoltaikanlagen spielen in einigen europäischen Ländern bereits heute eine nicht mehr zu vernachlässigende Rolle in der Stromversorgung.[159] In der Zwischenzeit wurde durch den enormen Ausbau eine bis vor Kurzem kaum berücksichtigte kritische Masse erreicht. Bisher mussten sich Wechselrichter[160] von Photovoltaikanlagen bei einer Überschreitung der Netzfrequenz[161] von 50,2 Hertz unverzügliche vom Netz trennen. Die ursprüngliche Idee dahinter ist durchaus nachvollziehbar und berechtigt. Kommt es jedoch zu einer ungeplanten Überschreitung, z. B. durch eine hohe dezentrale Einspeisung werden im Extremfall mehrere Gigawatt an Leistung zeitgleich abgeschaltet. Dadurch kann ein Leistungssprung entstehen, der deutlich höher ist als die europaweit vorgehaltene Primärregelleistung (Reserve). Wird diese Marke wieder unterschritten, so kommt es annähernd zu einer zeitgleichen Wiederzuschaltung der dezentralen Erzeuger. Dadurch kommt es zu einem Pendeleffekt und zu einer neuerlichen Überschreitung der Frequenz von 50,2 Hertz.[162] Die Netzfrequenz kann nicht mehr stabilisiert werden. Die Folgen wären wahrscheinlich katastrophal. Daher müssen in Deutschland die Wechselrichter der Photovoltaikanlagen ab 2012 durch „fehlertolerantere Systeme" nachgerüstet, bzw. ausgetauscht werden.[163] [164]

157 Vgl. „Die elektrotechnischen Grundlagen für die Planung der 380kV-Höchstspannungsleitung" URL: http://www.thueringen.de/imperia/md/content/tmwta/energie/gutachten_380-kv-trasse_technischer_teil.pdf [04.12.2011].

158 Information aus persönlichen Gesprächen mit Netzbetreibern.

159 Vgl. Abschnitt 4.3.4, Erneuerbare Energieträger.

160 Wechselrichter richten den produzierten Gleichstrom in Wechselstrom um, damit dieser in unserer herkömmlichen Infrastruktur (230V) verwendet bzw. in das öffentliche Stromnetz eingespeist werden kann.

161 Im zentraleuropäischen Verbundnetz standardmäßig 50 Hertz.

162 Vgl. „Das 50,2 Hz-Problem" URL: http://www.vde.com/de/fnn/arbeitsgebiete/tab/seiten/50-2-hz.aspx [01.12.2011].

163 Vgl. „Technische Anschlussbedingungen" URL: http://www.vde.com/de/fnn/arbeitsgebiete/seiten/n4105.aspx [01.12.2011].

164 Vgl. Oberste Priorität für Versorgungssicherheit: Verantwortung für sichere Energieversorgung muss auf allen Schultern verteilt werden URL: http://www.vbew.de/index.php?id=94&tx_ttnews%5Btt_news%5D=132&tx_ttnews%5BbackPid%5D=39&cHash=ba3ee51dd0 [25.11.2011].

Offensichtlich sind nicht nur Photovoltaikanlagen, sondern auch Blockheizkraftwerke und Windkraftanlagen davon betroffen.[165]

4.2.4 Intelligente Stromnetze

Unsere bisherige Stromversorgung ist auf relativ einfache Strukturen ausgelegt. Es gibt große, zentrale Erzeuger bzw. Großkraftwerke, ein Verteilungsnetz, u. U. Speicher (z. B. Pumpspeicherkraftwerke) und die Verbraucher. Dementsprechend wurde diese Infrastruktur auch geplant und aufgebaut. Der Vorteil einer zentralen Struktur ist ein verringerter Koordinierungsaufwand, welcher aber wiederum zulasten der Flexibilität geht.

Durch den verstärkten Einsatz von erneuerbaren Energien (insbesondere Sonnen- und Windenergie) und der damit einhergehenden, dezentralen Stromerzeugung, sowie durch ein komplexes Verbraucherverhalten, entstehen deutlich höhere Anforderungen an die Stromversorgungsnetze. Dies bedingt wiederum eine komplexe Netzwerksteuerung. Daher laufen derzeit die Vorbereitungen zur Implementierung von intelligenten Stromnetzen („Smart Grids“), wodurch die Komplexität der Infrastruktur erheblich steigen wird, da es zu einer verstärkten direkten Vernetzung und damit auch Abhängigkeit zwischen Strom- und (IKT) Steuerungsnetzen kommt. In der Fachwelt spricht man bereits von den größten IKT-Projekten, die in diesen Bereichen jemals durchgeführt wurden. Betrachtet man die sicherheitskritischen Entwicklungen in der IKT-Welt der vergangenen Monate, dann bedeutet das wohl eine erhebliche Herausforderung für die Zukunft, da die Stromversorgungssicherheit weiterhin gewährleistet werden muss.[166]

4.2.5 Intelligente Stromzähler

Obwohl die genauen Anforderungen an die intelligenten Stromnetze noch nicht beschrieben sind, wird schon eifrig an der Umsetzung eines möglichen Teilaspektes gearbeitet. Die Vorbereitung bzw. Einführung von intelligenten Stromzählern („Messcomputer“) statt der bisherigen mechanischen Ferrariszähler läuft auf Hochtouren.

Im Rahmen der Forschungsarbeit „*Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit*“[167] wurden erhebliche Bedenken zur derzeit geplanten Einführung von intelligenten Stromzählern festgestellt. Als größtes Manko wurden die fehlenden Risikoanalysen und Technikfolgenabschätzungen festgestellt.

Durch die bisherige Trennung des Stromnetzes von sonstigen öffentlichen Netzen ist ein relativ hohes Sicherheitsniveau gegeben. Durch die nunmehrige Absicht, IKT-Netze mehr oder weniger direkt mit dem Stromnetz zu verbinden, zumindest aber bisher in der IKT-Welt als unsicher geltende Systeme im Bereich der Stromnetze einzusetzen, ergibt sich eine völlig neue Situation. Diese wird mit dem Wissen, dass es auch in den jetzigen Stromnetzen ausreichend Schwachstellen gibt, welche jedoch so gut wie nicht ausgenutzt werden können, noch erheblich erschwert. Als Höhepunkt wird mit dem Smart Meter eine neue, in der derzeitigen Form wahrscheinlich als unsicher ein-

165 Vgl. „50,2 Hz Problematik betrifft nicht nur PV-Anlagen“ URL: http://www.bhkw-forum.info/nachrichten/5534/2011-11-24-502-hz-problematik-betrifft-nicht-nur-pv-anlagen/ [04.12.2011].
166 Vgl. Saurugg, 2011b, S. 7ff.
167 Saurugg, 2011b

zustufende Technologie in eine weitgehend ungesicherte Umgebung beim Endkunden als Netzeintrittspunkt eingebaut. Und soweit bisherige Untersuchungen vorliegen, scheint es zahlreiche Ansätze zu geben, wie diese Endgeräte manipuliert werden können. Im schlimmsten Fall ist damit zu rechnen, dass es gelingt, über das Endgerät direkt in das restliche Steuernetz vorzudringen. Die Folgen sind unabsehbar, die Folgekosten wären auf jeden Fall enorm. Daher wird mit der in der derzeitigen Form geplanten Implementierung von Smart Meter ein sehr gefährlicher Angriffsvektor[168] geschaffen.

Die Betriebssicherheit („safety“) von intelligenten Stromnetzen und -zählern hängt ganz wesentlich von der Angriffssicherheit („security“) ab. In der bisherigen Diskussion kommt die Angriffssicherheit und Risikobewertung weitgehend zu kurz. Als Gegenargument könnte gebracht werden, dass es schon zahlreiche Länder mit größeren Ausrollungen und Betriebserfahrung gibt, bis dato aber kaum größere Zwischenfälle bekannt wurden. Diesem ist mit den Erfahrungen aus der IKT-Welt zu entgegnen. Die Angriffe auf Computersysteme haben sich im Laufe der Jahre entwickelt und mittlerweile ein bedenkliches Ausmaß erreicht. Eine ähnliche Entwicklung muss auch im Bereich von intelligenten Stromzählern erwartet werden. Die Verwundbarkeit wird mit dem Umfang der Ausrollungen steigen. Einerseits, weil damit die Komplexität des Gesamtsystems steigt und auf der anderen Seite, weil sich damit für mögliche Angreifer lohnendere Ziele ergeben. Im Unterschied zur IKT-Welt sind aber bei einem Angriff auf die Strominfrastruktur die Folgen wesentlich verheerender und weitreichender. Bei der etablierten Strominfrastruktur können wir uns als Gesellschaft keine „Testphasen“ und ständiges Nachbessern, wie in der IKT-Welt, erlauben. Ganz im Gegenteil, das wäre grob fahrlässig.

Die Rolle von intelligenten Stromzählern ist für die Etablierung von intelligenten Stromnetzen nachrangig, wie auch aus einer aktuellen Analyse der deutschen Bundesnetzagentur hervorgeht:

> *„Smart Meter spielen bei der Intelligenzsteigerung der Verteilernetze eine untergeordnete Rolle. Sie sind weniger aus Netzerfordernissen, sondern eher für die verstärkte Marktteilnahme einzelner Kundengruppen erforderlich. Smart Meter dienen dazu, Reaktionen von Erzeugern (intelligente Einspeisezähler), Verbrauchern (intelligente Verbrauchszähler) und Dienstleistern auf Marktsignale in einem Smart Market zu ermöglichen.“*[169]

Daher ist in Anbetracht der dafür einzugehenden Sicherheitsrisiken eine umso kritischere Betrachtung erforderlich.

4.2.6 Elektromobilität

Derzeit gibt es umfangreiche Diskussionen zur Zukunft der Elektromobilität, worin eine große ökonomische und ökologische Chance gesehen wird. Damit wird aber auch die Komplexität der Stromnetze und -versorgung und die Fehlermöglichkeit weiter massiv ansteigen.

168 Benutzter Weg oder angewandte Technik eines Angreifers für das Eindringen in ein Computersystem.
169 Bundesnetzagentur, 2011b, S. 48.

Der möglicherweise zukünftige, verstärkte Einsatz von Elektroautos und der damit verbundene Anstieg am Strombedarf stellt an sich noch keine Ursache für ein Blackout dar. In Kombination mit den bisher aufgezählten Problembereichen, wie teil- bzw. zeitweise unzureichende Produktionskapazitäten, aber vor allem mit den bereits jetzt überlasteten Stromleitungen, wird das Risiko deutlich erhöht werden.[170] Ob dieses durch den möglichen Ansatz, Elektroautos in der Stehzeit als Stromspeicher bzw. als Puffer zu verwenden, kompensiert werden kann, muss erst verifiziert werden.[171]

Daher muss auch in diesem Bereich eine gesamtheitliche Betrachtung bereits in der frühen Planungsphase erfolgen. Der Fokus darf dabei nicht am Einzelsystem hängen bleiben. Umfassende Risikoanalysen sind unverzichtbar.

4.3 Organisatorische Faktoren

In diesem Abschnitt werden Faktoren beschrieben, die für ein Blackout relevant sein können und vor allem dem organisatorischen Bereich zuzuordnen sind. Eine ganz klare Trennung ist jedoch nicht möglich, da natürlich auch technische Aspekte eine Rolle spielen.

4.3.1 Das europäische Verbundsystem

Die europäischen Stromnetze sind in einem Verbundsystem zusammengefasst. Es besteht aus einem engmaschigen Hoch- und Höchstspannungsleitungsnetz zur Übertragung von elektrischer Energie. Der Verbund besteht aus mehreren physisch voneinander getrennten Netzen (z. B. Zentraleuropa, Großbritannien). Die Vernetzung im jeweiligen Teilbereich war bisher für die Stabilität des Gesamtnetzes sehr wichtig, da dadurch Reserven großräumiger eingesetzt werden konnten.[172] Jedoch wurde dazu bereits 2003 in Deutschland festgestellt:

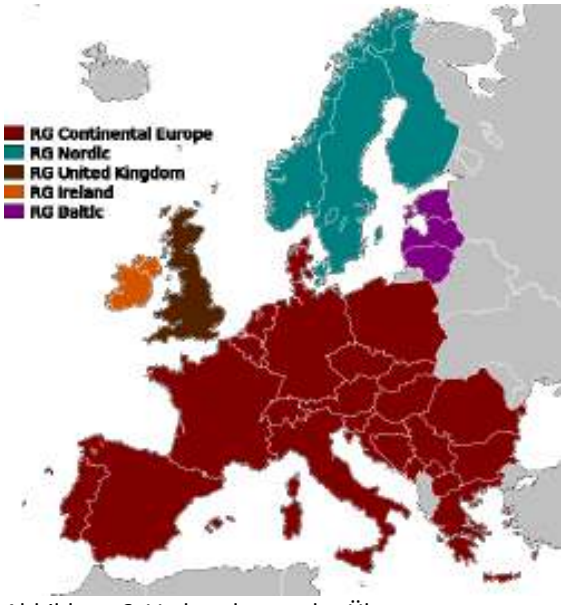

Abbildung 6: Verbundnetze der Übertragungsnetzbetreiber in Europa. Quelle: Wikipedia

> *„Es ist daher dringender denn je zu empfehlen, ein zukunftsfähiges Konzept für die Stromversorgung für die nächsten Jahrzehnte zu entwickeln, einen Ordnungsrahmen festzuschreiben und Entscheidungen zum Tätigen der dafür nötigen Investitionen umgehend zu treffen.“*[173]

170 Vgl. „Leistungsstarke Elektroautos belasten Stromnetz“ URL: http://www.drs.ch/www/de/drs/nachrichten/schweiz/314053.leistungsstarke-elektroautos-belasten-stromnetz.html [02.01.2012].

171 Vgl. „Wasserkraft soll verpuffenden Strom speichern“ URL: http://www.spiegel.de/wissenschaft/technik/0,1518,798495,00.html [18.11.2011].

172 Vgl. „Europäisches Verbundsystem: Rückgrat der Versorgungsqualität“ URL: http://www.vde.com/de/fg/ETG/Exklusiv-Mitglieder/Versorgungsqualitaet2007/Versorgungsqualitaet/Seiten/1-06.aspx [22.11.2011].

173 Vgl. ebenda, S. 63.

Fast 9 Jahre später werden aber noch immer die selben Forderungen vorgebracht.[174]

Der deutsche Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE) hält in einer 2003 erschienenen Analyse mehrerer großer Blackouts weiter fest:

> *„Ein Grundprinzip zur Kostenminimierung bei der Netzplanung ist die verbrauchernahe Erzeugung, um den Aufwand zur Energieübertragung und die dabei entstehenden Verluste so gering wie möglich zu halten. Kurze Übertragungswege wirken sich auch günstig auf die Stabilität und Spannungshaltung eines Netzes und damit letztlich auf die Versorgungszuverlässigkeit aus. (…) Eine Ausweitung der Transite belastet das Netz bis an seine Grenzen. (…) Eine wesentliche Ursache für die Blackouts bestand darin, dass die Netze bereits im Normalbetrieb hoch ausgelastet waren. (…) Die bereits bis an ihre Grenzen belasteten Leitungen werden im Störungsfall überlastet und automatisch abgeschaltet. (…) Investitionen in Stromnetze mit (vorgegebenen) Abschreibungsdauern von über 40 Jahren – gemessen an anderen Branchen extrem langfristige Kapitalbindungszeiträume – zwingen die Netzbetreiber zu sehr vorausschauendem Handeln. (…) Über große Entfernungen hoch ausgelastete Netze besitzen auch ein erhöhtes Risiko für großräumige kaskadenartige Ausbreitungen von Netzstörungen (Blackout). Auch ein umfangreicher Ausbau des Übertragungsnetzes kann die fehlende stabilitätsstützende Wirkung von Kraftwerkseinspeisungen, wenn diese sich womöglich in immer größeren Entfernungen befinden, nicht kompensieren. "*[175]

Diese Aussagen stehen klar im Widerspruch zu den heutigen Aktivitäten, die Übertragungsnetze massiv auszubauen, um vor allem den massiven Stromüberschuss vom Norden in den Süden von Deutschland zu transportieren.[176] Diese Änderung hängt eng mit dem Abschnitt 4.3.4, Erneuerbare Energieträger, zusammen. Der erforderliche Netzausbau und der Umbau in intelligente Stromnetze[177] erfordert enorme finanzielle Mittel und eine langfristige Investitionssicherheit, beides ist derzeit nicht ausreichend sichergestellt. Vor allem für die Investitionssicherheit sind klare politische Entscheidungen erforderlich. [178]

Es lässt sich daher ableiten, dass die europäischen Bürger in naher Zukunft deutlich mehr für die Stromversorgungssicherheit ausgeben werden müssen. Entweder direkt über höhere Stromkosten oder indirekt über Steuern und staatliche Zuschüsse. Alles andere würde zwangsläufig zu einer Verringerung der Versorgungssicherheit führen. Es stellt sich dennoch die Frage, ob die Aussage von 2003 nicht auch weiterhin Gültigkeit behalten hat und daher verstärkt in die Forschung zur lokalen Speicherfähigkeit von Energie investiert werden sollte.

174 Vgl. „Investitionen in die Infrastruktur als Schlüsselfaktor für den Energieumbau" URL: http://www.ots.at/presseaussendung/OTS_20111215_OTS0051/investitionen-in-die-infrastruktur-als-schluesselfaktor-fuer-den-energieumbau-bild [15.12.2011].

175 Vgl. VDE e.V., 2003, S. 57ff.

176 Vgl. „VDE-Studie: Overlay-Netz für beschleunigte Energiewende" URL: http://www.vde.com/de/verband/pressecenter/pressemeldungen/fach-und-wirtschaftspresse/seiten/2011-28.aspx [15.12.2011].

177 Vgl. Abschnitt 4.2.4 Intelligente Stromnetze

178 Vgl. „Investitionen in die Infrastruktur als Schlüsselfaktor für den Energieumbau" URL: http://www.ots.at/presseaussendung/OTS_20111215_OTS0051/investitionen-in-die-infrastruktur-als-schluesselfaktor-fuer-den-energieumbau-bild [15.12.2011].

Wie eng das (mittel)europäische Stromnetz bereits heute vernetzt und daher auch gegenseitig abhängig ist, lässt sich aus aktuellen Berichten ableiten. In Polen und Tschechien besteht die Befürchtung, dass deutscher Ökostrom durch enorme Überkapazitäten und Schwankungen in der Produktion das nationale Stromnetz destabilisiert bzw. die Wirtschaftlichkeit und Betriebsbereitschaft der eigenen Kohlekraftwerke massiv gefährdet. Es werden daher Stromimportsperren erwogen.[179] [180]Durch das kurzfristige Abschalten von zahlreichen deutschen Atomkraftwerken kann es vor allem in der kalten Jahreszeit zu Engpässen in der Stromversorgung kommen. Diese Engpässe sollen u. a. durch Importe aus Österreich[181] [182]abgefedert werden, obwohl Österreich gleichzeitig der größte Importeur von Strom aus Deutschland ist,[183] aktuell selbst massiv unter Wassermangel leidet und 2011 rund 20 % weniger Wasserstrom erzeugen konnte.[184] Die Trockenheit wirkt sich nicht nur auf Wasserkraftwerke aus, sondern auch auf Atomkraftwerke, die im schlimmsten Fall ihren Kühlwasserbedarf nicht mehr ausreichend decken können und ihre Leistung herunterfahren müssen. Besonders problematisch ist diese Situation derzeit in Frankreich, das gleichzeitig auch noch von Stromimporten aus Deutschland abhängig ist. Der Strom musste zur Stabilisierung des Netzes daher beim Jahreswechsel 2011/12 in einigen französischen Regionen rationiert werden.[185] Gleichzeitig herrscht in Mitteleuropa ein sehr milder Winter, welcher die Situation deutlich entlastet. Anfang Dezember 2011 mussten Kraftwerksreserven aus Österreich abgerufen werden. Starke Windenergieerträge im Norden von Deutschland und eine gleichzeitige, ungeplante Abschaltung eines süddeutschen Atomkraftwerkes machten diese Netzstabilisierungsmaßnahme erforderlich.[186]

Deutsche Industriebetriebe klagen bereits heute über eine zunehmende Unzuverlässigkeit der Stromversorgung.

> *„Kurze Unterbrechungen im Millisekundenbereich sowie Frequenzschwankungen sorgten jetzt häufiger als früher für Probleme. Die Stabilität komplexer Produkti-*

179 Vgl. „Polen gefährdet deutsche Energiewende“ URL: http://www.spiegel.de/wirtschaft/unternehmen/0,1518,801605,00.html [02.01.2012].

180 Vgl. „Deutsche Energiewende belastet tschechische Stromnetze“ URL: http://www.stromsparer.de/google/news/03590_deutsche-energiewende-belastet-tschechische-stromnetze.php [12.01.12].

181 Vgl. „Österreich will im Winter Strom liefern“ URL: http://www.focus.de/finanzen/news/energie-oesterreich-will-im-winter-strom-liefern_aid_670006.html [02.01.2012].

182 Vgl. „Energie: Österreich sichert Deutschland Strom“ URL: http://diepresse.com/home/wirtschaft/international/722064/Energie_Oesterreich-sichert-Deutschland-Strom?_vl_backlink=/home/wirtschaft/international/index.do [09.01.2012].

183 Vgl. „Deutschland bleibt Strom-Exporteur“ URL: http://www.spiegel.de/wirtschaft/unternehmen/0,1518,787387,00.html [02.01.2012].

184 Vgl. „Stromimport-Boom: Kraftwerken fehlt Wasser“ URL: http://kurier.at/wirtschaft/4460299-stromimport-boom-kraftwerken-fehlt-wasser.php [02.01.2012].

185 Vgl. „Frankreich: Angst vor dem Silvester-Blackout“ URL: http://diepresse.com/home/wirtschaft/international/720374/Frankreich_Angst-vor-dem-SilvesterBlackout?_vl_backlink=/home/wirtschaft/international/index.do [02.01.2012].

186 Vgl. „Österreich rettet deutsche Stromversorgung“ URL: http://www.welt.de/dieweltbewegen/article13798376/Oesterreich-rettet-deutsche-Stromversorgung.html [09.01.2012].

onsprozesse sei bedroht – lange bevor die Allgemeinheit einen Blackout bemerke." [187]

Derartige Zusammenhänge sollten zwangsläufig den Optimismus – „es wird schon nichts passieren" – trüben. Im Sinne des Kapitels Komplexe Systeme und die Stromversorgung sollten hier wohl keine Zweifel mehr bestehen, dass niemand in der Lage sein kann, diese komplexen Zusammenhänge zu durchschauen bzw. über die tatsächliche Ausfallsicherheit eine konkrete Aussage treffen zu können.

4.3.2 Das österreichische Stromnetz

In Österreich gibt es rund 10.000 kleine bis mittelgroße Stromausfälle pro Jahr. Die meisten davon - Unterbrechungen im Millisekundenbereich („Flackern") - sind für die gewöhnlichen Endkunden aufgrund der sehr kurzen Dauer nicht bzw. kaum wahrnehmbar. In der industriellen Fertigung können diese jedoch Auswirkungen zeigen. Die Unterbrechungen sind in der Regel lokal begrenzt und werden in durchschnittlich 70 Minuten behoben.[188] Auf alle Stromkunden gleichmäßig verteilt, ergab sich 2009 eine Stromunterbrechung von 36,7 Minuten.[189] In Deutschland betrug die Ausfallzeit sogar nur 16,5 Minuten.[190] Bei einer Zuverlässigkeit der bisherigen Stromversorgung mit annähernd 100 Prozent ist es durchaus nachvollziehbar, dass es kaum entsprechendes Problembewusstsein hinsichtlich möglicher Blackoutszenarien gibt.

Das derzeitige österreichische Übertragungsnetz ist großteils rund 60 Jahre alt. Der Stromverbrauch hat sich in dieser Zeit beinahe verfünffacht. Daher arbeitet dieses Übertragungsnetz bereits an seiner Leistungsgrenze. Insbesondere die Nord-Süd-Verbindungen sind massiv überlastet. Eine nachhaltige Entspannung soll durch den Lückenschluss des 380-kV-Ringes entstehen.[191] Ähnliche Szenarien gibt es auch in anderen Ländern. Durch diese permanente Überlastung stehen kaum Reservekapazitäten zur Verfügung, um beim Ausfall eines Teilstückes die Energie ohne Probleme auf andere Leitungen übertragen zu können.

4.3.3 Strommarktliberalisierung

Mit der von der EU forcierten Strommarktliberalisierung ab Ende der 1990er Jahre sollte ein reibungsloser Elektrizitätshandel zwischen den Mitgliedsstaaten umgesetzt werden. Die Energieversorgung gehörte bis dahin zu den Kernaufgaben des Staates und daher waren weite Teile der Stromproduktion und des Energienetzes fest in staatlicher Hand. Die ursprüngliche Intention, die Monopolstellung aufzubrechen und durch den freien Markt auch eine Preissenkung für die Verbraucher zu ermöglichen, ist mittlerweile weitgehend obligat. Auf der einen Seite wird die Möglichkeit eines

187 Vgl. URL: http://www.focus.de/immobilien/energiesparen/energiewende-produktion-von-solarstrom-waechst-rapide_aid_698044.html [09.01.2012].
188 Vgl. „BlackÖ.1" URL: http://www.energyefficiency.at/web/projekte/blacko.html [22.11.2011].
189 Vgl. „Österreich: Versorgungssicherheit gewährleisten" URL: http://oesterreichsenergie.at/die-versorgungssicherheit-in-oesterreich-ist-gewaehrleistet.html [22.11.2011].
190 Vgl. „Versorgungszuverlässigkeit" URL: http://www.vde.com/de/fnn/arbeitsgebiete/versorgungsqualitaet/seiten/versorgungszuverlaessigkeit.aspx [22.11.2011].
191 Vgl. „380-kV-Salzburgleitung" URL: http://www.verbund.com/cc/de/news-presse/aktuelle-projekte/oesterreich/380-kv-leitung [30.12.2011].

Stromlieferantenwechsels kaum in Anspruch[192] genommen und auf der anderen Seite bleiben immer weniger große Anbieter übrig, sodass die Preisunterschiede zunehmend sinken.[193] [194]

> *„Die forcierten Wettbewerbsbedingungen führen teilweise zu einem Kraftwerkseinsatz, der nicht mehr verbrauchernah ist und starken zeitlichen Änderungen unterworfen ist. Dies führt zu höheren internationalen Transporten und wechselnden Leistungsflüssen in den Netzen und damit zu höherer Belastung der Kuppelleitungen zu Nachbarnetzen. Hinzu kommt, dass Kraftwerke stillgelegt und an den betroffenen Standorten keine Erneuerungsinvestitionen getätigt werden."*[195]

Nachdem der Strommarkt nun marktwirtschaftlich ausgerichtet ist, müssen die Unternehmen auch Gewinne erwirtschaften. Dies bedeutet, dass erforderliche Investitionen nicht in jedem Fall umgesetzt, sondern hinausgeschoben werden.[196] Das ist zwar längerfristig ein Bumerang, beschert aber kurzfristige Gewinne. Diese Entwicklung konnte zumindest in einigen europäischen Ländern beobachtet werden. In diesem Zusammenhang spielt vor allem das Alter eines Teils der europäischen Stromnetzinfrastruktur eine Rolle. Teile davon sind durchaus 50 Jahre oder älter und erfordern daher eine entsprechende Wartung und Instandhaltung.

Die Vernachlässigung von Betriebsmitteln hinsichtlich Wartung und Erneuerung aus Gewinnstreben ist ein ständig wiederkehrender Vorwurf an die Elektrizitätsgesellschaften. Bisher werden vor allem in den USA größere Zwischenfälle damit in Zusammenhang gebracht.[197]

Ein anderer Vorwurf richtet sich von der Elektrizitätswirtschaft an die Politik. Durch den marktregulierenden Eingriff und die Aufsplittung des hochkomplexen Systems der Stromversorgung in möglichst viele Teile der Lieferkette, haben sich nicht zu vernachlässigende Risiken ergeben. So kann es nun vorkommen, dass jene Funktionen, die früher räumlich in einer Leitstelle zusammengefasst waren und ein eingespieltes Team bildeten, nun viele Kilometer voneinander getrennt sind. Darüber hinaus kann es etwa aus rechtlichen Gründen, wie z. B. bei Haftungsfragen, zu Verzögerungen oder gar Unterlassungen von Informationsübermittlungen kommen, weil die beteiligten Stellen nicht einer Organisation angehören.[198]

> *„Die Sicherheit eines Versorgungsnetzes hängt nicht alleine vom Betrieb des eigenen Netzes, sondern immer stärker von der Funktionsfähigkeit des vermaschten Gesamtnetzes ab. Der Informationsbedarf moderner Systembetreiber endet da-*

192 Vgl. „Stromanbieter wechseln" URL: http://www.konsument.at/cs/Satellite?pagename=Konsument/MagazinArtikel/Detail&cid=318873037003 [30.12.2011].
193 Vgl. „Strom-Lieferantenwechsel bringt in Österreich weniger als anderswo" URL: http://www.tt.com/csp/cms/sites/tt/Überblick/Wirtschaft/WirtschaftContainer/2767619-8/strom-lieferantenwechsel-bringt-in-österreich-weniger-als-anderswo.csp [30.12.2011].
194 Vgl. „Geschichte der Strommarktliberalisierung" URL: http://www.stromanbieter-wechseln.net/strommaerkte/geschichte-der-strommarktliberalisierung.html [30.12.2011].
195 Vgl. VDE e.V., 2003, S. 57.
196 Vgl. ebenda, S. 61.
197 Vgl. CRO Forum, 2011, S. 3.
198 Vgl. ebenda, S. 5.

her nicht an der Grenze des eigenen Versorgungsgebietes, sondern setzt Informationen über benachbarte Systeme und ihren Status voraus."[199]

Wie die bisherigen Beispiele gezeigt haben, ist aber besonders in Notfällen ein rasches und entschiedenes Handeln erforderlich, um folgenschwere Zwischenfälle zu verhindern. Es bleiben nur wenige Minuten zum Handeln, bevor das System außer Kontrolle gerät.

Es muss daher in Betracht gezogen werden, dass der finanzmarktorientierte Eingriff in das komplexe System der Stromversorgung langfristig negative Folgen für die Versorgungssicherheit nach sich ziehen könnte. Die überhastete Implementierung von intelligenten Stromzählern („Smart Meter") in das hoch komplexe System verstärkt diese Befürchtung.[200]

Marktmanipulationen durch Marktteilnehmer werden in dieser Arbeit nicht weiter berücksichtigt. Solche erfolgten etwa in den USA, wo künstliche Knappheiten erzeugt wurden, um den Strompreis zu erhöhen.[201]

4.3.4 Erneuerbare Energieträger

Erneuerbare Energieträger, wie etwa Wind-, Wasser- oder Sonnenenergie, spielen in Europa bereits heute eine nicht mehr vernachlässigbare Rolle in der Stromerzeugung. Großflächige Ausfälle, z. B. durch schneebedeckte Photovoltaik-Anlagen, Wassermangel oder fehlenden Wind, können rasch die vorgehaltenen Primärregelleistungen (Reserven) ausreizen, insbesondere nach der kurzfristigen Abschaltung zahlreicher Atomkraftwerke.[202]

„For example wind energy in East Germany during strong wind conditions can provide up to 12GW, which is more than all German coal and gas fired power plants considered together."[203]

Auch die unkontrollierte und plötzlich verstärkte Einspeisung von Strom aus Photovoltaikanlagen oder Windkraftwerken kann zur Destabilisierung des Stromnetzes führen.[204] Daher zahlen heute Stromlieferanten zum Teil schon Negativpreise, d. h. Großkunden werden dafür bezahlt, dass sie momentan überschüssigen und das Stromnetz destabilisierenden Strom verbrauchen.[205] Die wesentliche Herausforderung ist, dass die bisherigen Stromnetze stark hierarchisch geplant und errichtet und daher die dezentralen Einspeiser nicht berücksichtigt wurden.[206] Diese stellen beim weiteren Ausbau deutlich höhere Anforderungen an das Gesamtnetz, als bisher vorgesehen.[207]

199 Zeitung für kommunale Wirtschaft, 2003, S. 3.
200 Vgl. Saurugg, 2011b.
201 Vgl. „California electricity crisis" URL: https://secure.wikimedia.org/wikipedia/en/wiki/California_electricity_crisis [09.01.2012].
202 Vgl. „Stromimport-Boom: Kraftwerken fehlt Wasser" URL: http://kurier.at/wirtschaft/4460299.php [02.12.2011].
203 CRO Forum, 2011, S. 6.
204 Vgl. „Angst vor dem Blackout" URL: http://www.welt.de/print/wams/vermischtes/article13749772/Angst-vor-dem-Blackout.html [04.12.2011].
205 Vgl. CRO Forum, 2011, S. 6.
206 Vgl. „AMIS Power Snapshot Analyse" URL: https://www.youtube.com/watch?v=KNdYoapkikE [09.01.2012].
207 Vgl. Abschnitt 4.2.4, Intelligente Stromnetze.

Erneuerbare Energiequellen verfügen darüber hinaus über den Nachteil, dass sie nicht permanent zur Verfügung stehen. Daher sind zusätzliche Kraftwerke oder Speichermöglichkeiten erforderlich, die diese Lücken schließen können. Bisher wurde dies vor allem durch Atomkraftwerke bewerkstelligt, da diese relativ flexibel betrieben werden können. Kohlekraftwerke sind hingegen nicht für einen flexiblen Einsatz geeignet. Der Ausstieg aus der Atomenergie ist zu begrüßen, dennoch muss durch die kurzfristige Umsetzung mit einer zumindest temporären Destabilisierung der europäischen Stromversorgungssicherheit gerechnet werden. Diese Lücken könnten durch flexible Gaskraftwerke abgedeckt werden, aber diese befinden sich noch im Bau bzw. müssen erst geplant werden.[208] Es gibt auch noch Finanzierungsprobleme, da private – gewinnorientierte – Unternehmen kein großes Interesse daran haben, unwirtschaftliche Kraftwerke nur für den Ausnahmefall zu errichten und zu betreiben. Staatliche Zuschüsse scheitern, wie etwa in Bayern, an der EU-Wettbewerbskommission.[209] Auf der anderen Seite führt diese Vorgangsweise zur Quasi-Sozialisierung der Verluste und Risiken und zur Privatisierung der Gewinne und Vorteile.[210] Hier sind daher noch einige Hürden zu überwinden, um den Umstieg auf erneuerbare Energieträger erfolgreich umzusetzen. Nicht vergessen werden darf dabei, dass solche Reservekraftwerke auch Strom zum Hochfahren („Schwarzstartfähigkeit“) benötigen.[211]

Ein besonderer Fokus sollte daher auf den Ausbau von (lokalen) Speicherkapazitäten gerichtet werden.[212] Wahrscheinlich müssen dabei völlig neue Wege beschritten werden, um dieses Ziel im großen Stil zu erreichen.[213] Dieses Erfordernis kann aber zeitlich mit den sonstigen Entwicklungen nicht mithalten.

Daher gehen die derzeitigen Bemühungen vor allem in den Netzausbau, um z. B. den überschüssigen Windenergiestrom aus der Nordsee in die energiehungrigen Industrieregionen im Süden von Deutschland zu transportieren.[214] Dass eine hohe Dringlichkeit zur raschen Umsetzung von stärkeren Übertragungsleitungen („Stromautobahnen“) besteht, lässt sich nicht nur auch aus einer in Bearbeitung befindlichen EU-Verordnung ableiten. Diese sieht für die Planung und Genehmigung wichtiger europäischer Gas- und Stromleitungen eine Verkürzung auf drei Jahre vor. Bisher dauerten diese Verfahren in vielen Ländern häufig länger als 10 Jahre.[215] Derzeit müssen die Windenergiekraftwerke in Norddeutschland immer häufiger abgeschaltet werden, damit es zu keinen Netzdestabilisierungen kommt.[216]

208 Vgl. „"Energiewende": Der Blackout rückt näher“ URL: http://ef-magazin.de/2011/12/26/3331-energiewende-der-blackout-rueckt-naeher [02.01.2012].
209 Vgl. „Achtung, falscher Atomalarm!“ URL: http://www.wissen.de/wde/generator/wissen/services/nachrichten/ftd/PW/60148073.html [02.01.2012].
210 Vgl. Abschnitt 3.6.5, Technikfolgenabschätzung – Sicherheitsvorschriften und Kontrolle
211 Vgl. Prillwitz/Krüger, 2007.
212 Vgl. „AMIS Power Snapshot Analyse“ URL: https://www.youtube.com/watch?v=KNdYoapkikE [09.01.2012].
213 Vgl. CRO Forum, 2011, S. 2.
214 Vgl. „Netzbetreiber planen riesige Stromautobahnen“ URL: http://www.focus.de/immobilien/energiesparen/energie-netzbetreiber-planen-riesige-stromautobahnen_aid_668241.html [02.01.2012].
215 Vgl. „EU-Kommission plant das Super Grid“ URL: http://www.euractiv.de/energie-und-klimaschutz/artikel/eu-kommission-plant-europaische-energie-infrastruktur-003729 [05.10.2011].
216 Vgl. „Windenergie-Chef wirft Netzbetreibern Blockade vor“ URL: http://www.welt.de/wirtschaft/energie/article13695438/Windenergie-Chef-wirft-Netzbetreibern-Blockade-vor.html [02.01.2012].

Der immer häufiger werdende Windenergieüberschuss in Norddeutschland, der aufgrund der fehlenden Transportleitungen nicht abtransportiert werden kann, führt dazu, dass die Kraftwerke abgeschaltet werden müssen.[217]

Erneuerbare Energiequellen und eine dezentrale Energieversorgung, wie etwa durch Blockheizkraftwerke (BHKW), können aber auch heute schon bei entsprechenden Vorkehrungen für den Inselbetrieb einen bedeutenden Beitrag zur dezentralen Widerstandsfähigkeit von wichtigen Anlagen beisteuern.[218] Die ebs Hauptkläranlage Wien GesmbH hat beispielhaft erst vor Kurzem diesen wichtigen Schritt gesetzt. Bis 2020 soll der enorme Eigenenergieverbrauch[219] durch Rückgewinnung der brennbaren Gase aus dem anfallenden Klärschlamm und der Verwertung in einem eigenen Blockheizkraftwerk, weitgehend autark sichergestellt werden können. Ein Beispiel dafür, dass eine dezentrale Stromversorgungsinfrastruktur sehr wohl sinnvoll und zielführend ist, wenngleich eine zusätzliche Vernetzung unerlässlich bleiben wird. [220]

4.3.5 Der deutsche Ausstieg aus der Atomenergie

Wie bereits mehrfach angesprochen, ist der kurzfristige deutsche Ausstieg aus der Atomenergie nicht unproblematisch. Die deutsche Bundesnetzagentur[221] veröffentlichte hierzu im Mai 2011 eine Aktualisierung zum Bericht "Auswirkungen des Kernkraftwerk-Moratoriums auf die Übertragungsnetze und die Versorgungssicherheit". Diese enthält ganz klare Hinweise auf die möglichen negativen Folgen, deren Tragweite erst in der Zusammenschau mit den sonstigen Analysen in dieser Arbeit bewusst werden.

> *„Die historisch einmalige zeitgleiche Abschaltung von 5.000 MW Leistung und das längerfristige Fehlen von 8.500 MW Leistung bringen die Netze an den Rand der Belastbarkeit. Das Fehlen dieser Leistung führt dazu, dass in sehr vielen Zeiten der Markt über die entsprechenden Handelsgeschäfte und die Prognosen der Einspeisung erneuerbarer Energien eine Situation, d. h. einen Kraftwerkseinsatz verursacht, der einen (n-1)-sicheren Netzbetrieb nicht ermöglicht." (…)*
>
> *Das erhebliche netztechnische Problem, das mit dieser Marktkorrektur verbunden ist, besteht darin, dass das genannte Maßnahmenpaket eigentlich für Ausnahmesituationen wie Ausfälle von Kraftwerken oder Leitungen gedacht ist, nunmehr aber oft bereits für den Normalfall eines intakten Netzes nahezu vollständig ausgeschöpft wird und damit bei zusätzlichen unerwarteten Notfällen nicht mehr zur Verfügung steht. Damit steigt das Risiko der Nichtbeherrschbarkeit von Störungsfällen im Netz deutlich an. (…)*

217 Vgl. „Stromnetz bremst Windkraft aus" URL: http://www.ftd.de/politik/deutschland/:engpass-bei-energieversorgung-stromnetz-bremst-windkraft-aus/60123011.html [09.01.2012].

218 Vgl. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 8 und S. 14.

219 Verbrauch von ca. 20.000 Haushalten

220 Vgl. „Kooperation Wien Energie und Hauptkläranlage Wien" URL: http://www.wienerstadtwerke.at/eportal/ep/contentView.do/contentTypeId/1001/channelId/-30566/programId/13111/pageTypeId/11083/contentId/27784 [16.12.2011].

221 „Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen ist eine selbständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft und Technologie." URL: http://www.bundesnetzagentur.de [03.01.2012].

Es ergibt sich die paradoxe Situation, dass durch das Moratorium ein Mehr an Transportkapazitäten erforderlich wird und gleichzeitig Netzumbau- oder Netzverstärkungsmaßnahmen aufgrund der erhöhten Netzbelastung nicht mehr wie geplant durchgeführt werden können. (...)

Bei einer dauerhaften Stilllegung der acht Kernkraftwerke des Moratoriums kann Deutschland schon heute nicht mehr im bisherigen Umfang als eine der Stützen der Versorgungssicherheit im europäischen Verbund auftreten. Dies ist im Hinblick darauf, dass Nachbarländer auf den deutschen Export gebaut und sich darauf verlassen haben, nicht unproblematisch. (…)

Aus Sicht der Übertragungsnetzbetreiber entsteht bei gleichgerichteten weiträumigen Transportkorridoren infolge lastferner Erzeugung ein erhöhtes Risiko kaskadierender und damit großflächiger überregionaler Auswirkungen bei außergewöhnlichen Fehlerereignissen, falls bei Ausfall eines zentralen Leitungssystems der Lastfluss von anderen, ebenfalls bereits stark ausgelasteten Leitungen aufgenommen werden muss. Es ist erwartbar, dass derartige Fehler in Deutschland auch Auswirkungen auf die europäischen Nachbarregelzonen hätten. [222]

Die Aussagen stammen von einer öffentlichen Behörde. Daher darf davon ausgegangen werden, dass diese nicht von wirtschaftlichen Interessen beeinflusst ist und annähernd die Realsituation beschrieben wird.

4.4 Sonstige Faktoren

4.4.1 Koronaler Massenauswurf (KMA)

Bei einem KMA (englisch Coronal Mass Ejection/CME) handelt es sich um eine Sonneneruption, bei der riesige Mengen elektrisch geladener Gase (Plasmawolken) in den Weltraum hinausgeschleudert werden. Wenn diese Gase Richtung Erde geschleudert werden, wird das Erdmagnetfeld stark deformiert und die von der Sonne kommenden Teilchen fließen als elektrischer Strom in Spiralbahnen zu den Polen der Erde, wo sie Polarlichter auslösen. Diese Teilchen benötigen etwa 24 bis 36 Stunden, um auf die Erde zu treffen. Die Wirkung dauert etwa 24 bis 48 Stunden an. Je nach Stärke des Sonnensturms und der auftreffenden Teilchen können durch induzierte Überspannungen Schäden an Satelliten, Störungen im Funkverkehr (inkl. GPS Navigation) oder im schlimmsten Fall Blackouts verursacht werden.[223] [224]Im März 1989 wurde in Kanada ein mehrstündiges Blackout verursacht, von dem 6 Millionen Menschen betroffen waren. Dabei wurden zum Teil Stromnetze und elektrische Geräte zerstört. Der Großteil der heutigen Informations- und Kommunikationstechnikinfrastrukturen wurde aber erst in den vergangenen 25 Jahren etabliert. Daher können wir die möglichen Folgen eines solchen Zwischenfalls heute gar nicht richtig erfassen oder beurteilen. Was wir sicher wissen ist, dass nach einer langen Phase an relativer Inaktivität die Aktivität der

222 Bundesnetzagentur, 2011a, S. IVff.

223 Vgl. „Sonnensturm droht weltweit Stromnetze lahmzulegen“ URL: http://www.welt.de/wissenschaft/article13418284/Sonnensturm-droht-weltweit-Stromnetze-lahmzulegen.html [19.06.2011].

224 Vgl. „Die spinnen, die Kompasse“ http://www.wienerzeitung.at/themen_channel/wzwissen/technologie/51350_Die-spinnen-die-Kompasse.html [30.11.2011].

Sonne in den vergangenen Monaten deutlich gestiegen ist. Die NASA erwartet in den nächsten Jahren deutlich erhöhte Sonnenaktivitäten.[225] [226] [227]

4.4.2 Mangelndes Risikobewusstsein

Das Deutsche Rote Kreuz gab 2008 eine Umfrage mit der Frage:

> *„Stellen Sie sich bitte vor, es gäbe 14 Tage Stromausfall. Das bedeutet unter anderem, kein Geld aus dem Bankomat, kein Sprit an der Tankstelle, keine Kühlung im Supermarkt. Glauben Sie, Sie wären in der Lage, sich selbst zu versorgen?“*

in Auftrag. Auf diese Frage antworteten von 1.000 Befragten 76 Prozent mit Ja. Dieses Ergebnis wurde als „eine trügerische Annahme“ und Selbstüberschätzung, die auf einem völligen Mangel an Information und daher auf mangelndem Risikobewusstsein gründet, zurückgeführt. Die Einsatzorganisation sieht die Lage realistischer und geht davon aus, dass das öffentliche Leben in kürzester Zeit zusammenbrechen und chaotische Zustände ausbrechen würden. Die Handlungsfähigkeit der Einsatzorganisationen würde sich dabei auf wenige Stunden beschränken.[228]

Eine Studie im Herbst 2005 zum Blackout im Münsterland kommt zu ähnlichen Feststellungen. Darin wird u. a. die Wichtigkeit von laufend aktualisierten und adaptierten staatlichen Konzepten für die Notfallversorgung im öffentlichen wie auch im privaten Bereich, festgehalten. Die im Kalten Kriege vorhandenen Eigenvorsorgemaßnahmen, wie etwa die Eigenbevorratung, werden heute von vielen Menschen als überholt gesehen, was jedoch trügerisch und falsch ist.[229]

Eine weitere Erkenntnis dieser Studie lautet, dass sich die Erwartungshaltungen zwischen den Behörden und der Bevölkerung nicht decken. Die Erwartungshaltung an die BOS ist zu hoch und gleichzeitig fehlt es massiv an der Selbsthilfefähigkeit der Bevölkerung. Eine Verbesserung der Information und Aufklärung der Bevölkerung (Risikokommunikation) ist daher zwingend erforderlich. Im Rahmen von Umfragen wurde festgestellt, dass es durchaus die Bereitschaft und das erforderliche Interesse an Themen zur Selbsthilfe und zur Notfallvorsorge bei der Bevölkerung gibt.[230]

Die Studie kommt daher zum Schluss, dass Politik, Verwaltung und die mit Aufgaben des Katastrophenschutzes beauftragten Organisationen in der Bevölkerung das Bewusstsein für die Notwendigkeit privater Notfallvorsorge fördern müssen. Derzeit verlassen sich zu viele Menschen ausschließlich auf die öffentliche Hilfe, wie etwa von Hilfsorganisationen oder staatlichen Stellen, anstatt entsprechende Eigenverantwortung und Eigenvorsorgemaßnahmen zu übernehmen.[231]

Wir sind heute an unsere ziemlich komfortablen Lebensumstände so gewöhnt, dass wir nicht darüber nachdenken bzw. uns einen anderen Zustand gar nicht vorstellen

225 Vgl. „Blackout: The Sun-Earth Connection“ URL: http://sunearth.gsfc.nasa.gov/podcasts/media/Blackout/Blackout_part1.htm [04.12.2011].
226 Vgl. CRO Forum, 2011, S. 13.
227 Vgl. Centra Technology, Inc., 2011.
228 Vgl. „Großkatastrophe Stromausfall: Deutsche wiegen sich in Sicherheit“ URL: http://www.drk.de/pressemeldungen/meldung/5886-groaykatastrophe-stromausfall-deutsche-wiegen-sich-in-sicherheit.html [22.11.2011].
229 Vgl. Fachhochschule Münster, 2008, S. 77ff.
230 Vgl. ebenda, S. 78.
231 Vgl. Fachhochschule Münster, 2008, S. 80.

können oder wollen. Ständig vorhandene Gefahren, wie ein teilweiser bis gänzlicher Ausfall unserer gewohnten Infrastruktur im tiefsten Frieden, werden nicht wahrgenommen oder aus dem Denken ausgeblendet.

4.5 Zusammenfassung

Ziel dieses Kapitels ist die Sensibilisierung des Lesers hinsichtlich der Bedeutung eines möglichen temporären Ausfalls der Stromversorgung. Eine für uns alle selbstverständliche, da bisher weitgehend permanent vorhandene, lebenswichtige Ressource. Dabei sollten vor allem die großen Abhängigkeiten, die steigende Komplexität und die damit einhergehende Verwundbarkeit, vor Augen geführt werden.

In den vergangenen Monaten kann eine stetig steigende Anzahl von Meldungen von eventuell zu erwartenden Blackouts in Europa beobachtet werden. Es besteht durchaus die Möglichkeit, dass dieses Thema dazu genutzt wird, um mehr Ressourcen, etwa für den Netzausbau, zu lukrieren.[232] Trotz allem sind die derzeit stattfindenden kritischen Veränderungen in der bestehenden Strominfrastruktur nicht wegzuleugnen. Dies wird auch durch eine Anfang 2012 erschienene Analyse der deutschen Bundesnetzagentur festgehalten: „Der hierfür notwendige Umbau des Versorgungssystems erfolgt dabei am 'offenen Herzen', nämlich im Vollbetrieb und aus Netzperspektive zunehmend an seiner Grenze.“[233]

Die Folgen sind gegenwärtig noch nicht absehbar, jedoch bergen sie konkrete Risiken für größere Netzausfälle in sich. Es ist daher eine steigende Anzahl von (Teil)Blackouts zu erwarten. Dies inkludiert, dass Netzbetreiber in Krisensituationen Teilbereiche des Netzes abschalten können, um das Gesamtnetz wieder zu stabilisieren.

Der Stand der Vorbereitungen auf Blackouts ist in Österreich, wie auch in vielen anderen europäischen Ländern, sehr heterogen. Generell muss davon ausgegangen werden, dass die Netzbetreiber und EVUs alles daran setzen werden, mögliche Blackouts zu verhindern. Dennoch kann eine solche Krisenprävention nicht alleine den EVUs überlassen werden. Nach wie vor gehen viele Akteure davon aus, dass es zu keinem lang andauernden und überregionalen Stromausfall kommen wird. Dabei sind ihnen weitgehend weder die Komplexität eines solchen Stromausfalls noch die wechselwirksamen Abhängigkeiten der Infrastrukturen bekannt oder tatsächlich bewusst. Vor allem die Bevölkerung in städtischen Gebieten ist auf ein solches Szenario nicht vorbereitet. Die Selbstschutz- oder Selbsthilfepotenziale werden weitgehend nicht genutzt und auch nicht gefördert. Auch sonstige Institutionen wie Wirtschafts- und Industriebetriebe und Behörden sind höchst unterschiedlich vorbereitet. Derzeit fehlt es vor allem an einem gesamtstaatlichen, nachhaltigen Risiko- und Krisenmanagement. Bei derart schwerwiegenden möglichen Konsequenzen muss die Prävention absolut im Vordergrund stehen. Daher ist es erforderlich, dass sowohl die Risikosteuerung als auch das Krisenmanagement von einer sektoralen zu einer prozessualen Betrachtung führen. Der Fokus auf Einzelsysteme führt in die Sackgasse mit verheerenden Folgen.[234]

232 Vgl. „Netzagentur-Chef warnt vor Blackout-Panik“ URL: http://www.spiegel.de/wirtschaft/unternehmen/0,1518,758403,00.html [22.11.2011].

233 Vgl. Bundesnetzagentur, 2011b, S. 47.

234 Vgl. Zukunftsforum öffentliche Sicherheit, 2008, S. 26.

Zur Warnung vor der möglichen Überschätzung von Bewältigungskapazitäten sollte das aktuelle Beispiel eines Stromausfalles im Bereich der Deutschen Bahn herangezogen werden. Am 15.Dezember 2011 brach infolge eines missglückten Notstromversorgungstests der Berliner Bahnverkehr für mehrere Stunden zusammen. Bereits fünf Jahre zuvor gab es einen ähnlichen Zwischenfall. Diese Tests wurden aus Kostengründen am Tag durchgeführt – eine folgenschwere und teure Fehlentscheidung. Auf der anderen Seite werden wohl einige Ableitungen zum Thema Blackout damit bestätigt. Nur weil etwas vorgesehen ist, bedeutet das leider noch lange nicht, dass im Anlassfall alles reibungslos funktioniert.[235]

Unrealistische Annahmen basierend auf der mangelnden Kommunikation zwischen den verschiedenen Akteuren sind ein nicht zu vernachlässigender Faktor. Risiko- und Krisenmanagement müssen daher auf allen Ebenen standardisiert werden. Entsprechende Übungen sind dabei das um und auf, damit mögliche Irrtümer und Probleme rechtzeitig erkannt bzw. das Schlüsselpersonal auf außergewöhnliche Situationen vorbereitet werden.[236]

Das Szenario Blackout ist ein Schlüsselszenario. Es besitzt Wechselwirkungen mit so gut wie allen anderen lebenswichtigen Infrastrukturen und hat Auswirkungen auf nahezu alle Lebens- und Geschäftsbereiche. Sollte es zu einem solchen überregionalen und lang anhaltenden Stromausfall kommen, wird dies erhebliche Beeinträchtigungen für die Bevölkerung und enorme volkswirtschaftliche Schäden nach sich ziehen. Die Sicherheit und die Grundversorgung der Bevölkerung könnten von staatlichen Einrichtungen und privaten Hilfsorganisationen nicht mehr aufrechterhalten werden. Ein Stromausfall dieser Größenordnung wäre eine nationale Katastrophe mit kurz-, mittel- und langfristigen Schäden für alle Bereiche der Gesellschaft.[237]

Daher ist auch jeder Einzelne gut beraten, Eigenverantwortung zu übernehmen und Eigenvorsorgemaßnahmen zu treffen. Für die staatlich organisierte Hilfe sind weitere Analysen durchzuführen und entsprechende Konsequenzen daraus abzuleiten.

Die westlichen, technisierten Gesellschaften wenden für diverse Maßnahmen zur Erhöhung der allgemeinen Sicherheit sehr viel Geld auf. Beispielsweise seien hier die Maßnahmen zum Schutz vor Terrorismus angeführt. Vergleicht man diese beiden Szenarien, dann steht der derzeitige Aufwand in keinem Verhältnis dazu. Jedes Opfer eines möglichen Terroranschlages ist zu viel. Aber im Vergleich dazu, mit wie vielen Betroffenen und mit welch hohen Schäden bei einem Blackout zu rechnen ist, wird dieses mögliche Szenario noch sehr nachlässig behandelt. Es sollte nicht erst zu einem Ereignis kommen müssen, um hier Änderungen herbeizuführen. Daher sind alle Verantwortungsträger auf allen Ebenen aufgefordert, sich mit diesem Katastrophenszenario auseinanderzusetzen. Das Eintreten eines Blackouts nach mangelhafter Vorbereitung auf dessen Bewältigung würde einen massiven Vertrauensverlust in die verantwortlichen Stellen nach sich ziehen.

„Die Vorsicht ist einfach, die Hinterdreinsicht vielfach“, Johann Wolfgang von Goethe

235 Vgl. „Zusammenbruch mit Vorankündigung“ URL: http://www.berliner-zeitung.de/berlin/s-bahn-zusammenbruch-mit-vorankuendigung,10809148,11345110.html [31.12.2011].

236 Vgl. Zukunftsforum öffentliche Sicherheit, 2008, S. 26f.

237 Vgl. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011.

5 Der Zivilschutz in Österreich

In diesem Kapitel wird das derzeitige Konzept des staatlichen Krisen- und Katastrophenschutzmanagements in Österreich (Zivilschutz) beleuchtet. Der Fokus richtet sich dabei auf Bewältigung eines Blackouts. Eine tiefer gehende Analyse ist im Rahmen der Masterarbeit geplant, die den Arbeitstitel „Krisenmanagement in außergewöhnlichen Schadenslagen am Beispiel Blackout und IT-Krisen“ trägt.

5.1 Zivil-/Bevölkerungsschutz

In Österreich wird nach wie vor der Begriff „Zivilschutz“ für den Bevölkerungsschutz verwendet, welcher als Gegenstück zum militärischen Anteil der Umfassenden Landesverteidigung (ULV) in den 1970er Jahren entstanden ist.

In anderen Ländern, wie etwa in der Schweiz oder Deutschland, wird heute der Begriff Bevölkerungsschutz[238] verwendet. Eine weitere Besonderheit in Österreich ist, dass es keine eigenen Einsatzmittel oder Organisationen für diese Aufgabe gibt. In Deutschland gibt es zum Beispiel ein eigenes Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)[239] sowie als operative Organisation das Technische Hilfswerk (THW[240]). In der Schweiz gibt es das Bundesamt für Bevölkerungsschutz (BABS[241]). Die operativen Fähigkeiten werden in den fünf Partnerorganisationen, Polizei, Feuerwehr, Gesundheitswesen, technische Betriebe und Zivilschutz abgebildet.[242]

Nach dem Ende des Kalten Krieges verfiel der militärische Bezug und damit auch weitgehend das Bewusstsein der Bevölkerung für die Notwendigkeit eines Selbstschutzes und einer Eigenvorsorge. Derzeit wird Zivilschutz praktisch Synonym für Katastrophenschutz verstanden.[243]

> *„Zivilschutz umfasst Aktivitäten zur Bewältigung von Katastrophen und Krisensituationen unterschiedlichster Art. Er umfasst*
> - *Maßnahmen des Selbstschutzes,*
> - *Maßnahmen der alltäglichen Gefahrenabwehr,*
> - *Maßnahmen zum Schutz vor Naturkatastrophen und technischen Unglücksfällen, ebenso wie*
> - *Vorsorgen zum Schutz vor möglichen Auswirkungen des internationalen Terrorismus.“*[244]

5.1.1 Zwei Ebenen Modell

Das österreichische Krisen- und Katastrophenschutzmanagement wurde 2003 neu organisiert. Dabei wurden zwei Ebenen festgelegt. Auf der ersten Ebene erfolgt die Katastrophenhilfe der Bundesländer, die direkte Gefahrenabwehr. Die zweite Ebene bil-

238 Im englischen „civil protection“
239 „Bundesamt für Bevölkerungsschutz und Katastrophenhilfe“ URL: http://www.bbk.bund.de [18.12.2011].
240 „Bundesanstalt Technisches Hilfswerk“ URL: http://www.thw.de [18.12.2011].
241 „Bundesamt für Bevölkerungsschutz“ URL: http://www.bevoelkerungsschutz.ch/ [01.01.2012].
242 Vgl. „Verbundsystem Bevölkerungsschutz“ URL: http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/Verbundsystem.html [01.01.2012].
243 Vgl. Bundesministerium für Inneres , 2010, S. 27f.
244 „Zivilschutz in Österreich“ URL: http://www.bmi.gv.at/cms/BMI_Zivilschutz/ [01.01.2012].

det das „Staatliche Krisen- und Katastrophenschutzmanagement“ (SKKM), welches im Bundesministerium für Inneres (BMI), Abteilung II/4,[245] angesiedelt ist.

> *„Die Koordinationszuständigkeit des BM.I umfasst demnach den Aufgabenbereich des Bundes im Krisen- und Katastrophenschutzmanagement, nicht jedoch den Aufgabenbereich der Länder.“*[246]

Zusätzlich gibt es einen Koordinationsausschuss unter dem Vorsitz des Generaldirektors für die öffentliche Sicherheit.

> *„In diesem Koordinationsausschuss sind alle Bundesministerien und Bundesländer, Einsatzorganisationen und Medien vertreten; ihm obliegt bei großräumigen Gefährdungslagen die Koordination und Abstimmung der auf Bundes- und Landesebene erforderlichen Maßnahmen. Der Ausschuss wird nicht nur im Anlassfall, sondern vor allem auch in der Grundsatzplanung koordinierend tätig. (…) Aufgabe des SKKM ist es, im Falle länger dauernder und komplexer Krisen- und Katastrophensituationen die rasche Koordination der Bundesbehörden untereinander sowie die Koordination und Zusammenarbeit mit den Ländern sicher zu stellen.“*[247]

Unmittelbar durch die Bundesverwaltung werden derzeit nur Sicherungsmaßnahmen nach dem Strahlenschutz- bzw. Epidemiegesetz vollzogen. Grundsätzlich ist es jedoch möglich, dass der jeweilige Bundesminister als oberste Behörde schon in erster Instanz zum Zwecke der Gefahrenabwehr einschreitet.[248] Im Fall eines österreichweiten oder großräumigen Blackouts würde der Bundesminister für Wirtschaft, Familie und Jugend (BMWFJ) automatisch zum Einsatzleiter werden.[249]

5.2 Katastrophen(schutz)management

Das Katastrophen(schutz)management ist ein permanenter Prozess mit den vier Phasen (siehe Abbildung 7):

- Vorsorge
- Bewältigung
- Wiederherstellung
- Vermeidung

Abbildung 7: Quelle: BMI, 2011, S. 17.

Das strategische Ziel des SKKM liegt dabei bei der bestmöglichen Verhinderung von Katastrophen. Dies soll durch Prävention und Risikooptimierung erfolgen, und bis 2020 optimiert werden.[250]

245 Vgl. „Zivilschutz in Österreich“ URL: http://www.bmi.gv.at/cms/BMI_Zivilschutz/mehr_zum_thema/Abteilung_II4.aspx [20.12.2011].
246 Bundesministerium für Inneres , 2010, S. 89.
247 Vgl. „Zivilschutz in Österreich“ URL: http://www.bmi.gv.at/cms/BMI_Zivilschutz/mehr_zum_thema/SKKM.aspx [20.12.2011].
248 Bundesministerium für Inneres , 2010, S. 89f.
249 Gem. Aussage Referatsleiter Referat II/4/a „Staatliches Krisen- und Katastrophenschutzmanagement sowie Zivilschutz“, BM.I/SKKM
250 Vgl. Bundesministerium für Inneres , 2011, S. 17.

Ein generelles Ziel ist die Förderung des Selbstschutzgedankens durch laufende Information und Aufklärung durch die Behörden und Zivilschutzverbände[251] auf Bundes- und Landesebene.

5.2.1 Einheitliche Begriffe – ÖNORM

Seit 2011 steht die ÖNORM S 2304:2011 07 15 zur Verfügung,[252] welche die Begriffe im Katastrophenmanagement[253] in Österreich vereinheitlichen soll. Ziel ist die Sicherstellung der gebotenen Interoperabilität und die Verbesserung der Zusammenarbeitsfähigkeit zwischen den unterschiedlichen (Einsatz-)Organisationen.[254]

5.2.2 Subsidiaritätsprinzip

Das österreichische Krisen- und Katastrophenschutzmanagement baut auf die primäre Selbsthilfe in lokalen Strukturen sowie auf dem Prinzip der subsidiären Intervention auf höheren Verwaltungsebenen auf.[255]

> Subsidiaritätsprinzip: *„Das Subsidiaritätsprinzip besagt, dass die einzelne, unmittelbarste Gemeinschaft möglichst viel Eigenverantwortung übernehmen soll und nur wenn es Aufgaben alleine nicht mehr erfüllen kann, auf die Hilfe der größeren Gemeinschaft zurückgreifen kann. Für die Städte und Gemeinden heißt das, dass sie über lokale Themen auch lokal entscheiden.“*[256]

Daher ist der erste Katastrophenschutzbehördenleiter der Bürgermeister, gefolgt vom Leiter der Bezirksverwaltungsbehörde und in letzter Instanz der Landesregierung. Eine Leitung auf Bundesebene ist nicht vorgesehen.

> *„Im föderalen österreichischen Verwaltungssystem ist aufgrund der Kompetenzverwaltung darüber hinaus eine Katastrophen-Einsatzleitung auf Bundesebene nicht möglich. Die Koordination bzw. Kooperation der Bundesländer untereinander erfolgt bei Großkatastrophen auf freiwilliger Basis im Wege der Landeswarnzentralen bzw. der Landesverbände und Dachverbände der Einsatzorganisationen.“*[257]

Die Bundesebene wird nur bei den überregionalen Gefährdungslagen „nuklearer Notfall“ und „Pandemie“ aktiv.

> *„In Österreich endet dieser behördliche 'Instanzenzug' in der Regel auf Landesebene. Gesetzliche Zuständigkeiten des Bundes bestehen auch bei Bundesländer übergreifenden Ereignissen nur hinsichtlich spezieller Materien, eine gesetzliche Koordinationszuständigkeit des Bundes besteht nicht im Wirkungsbereich der Länder.“*[258]

251 „Der Österreichische Zivilschutzverband“ URL: http://www.zivilschutzverband.at [18.12.2011].
252 Diese ÖNORM lag bei der Erstellung der Arbeit nicht vor und wurde auch erst in der Schlussphase entdeckt. Daher findet sie in dieser Arbeit keine Berücksichtigung. Eine nähere Betrachtung und Berücksichtigug wird in der Masterarbeit erfolgen.
253 Diese Normierung soll auch im Management von Krisen, Großschadensereignissen, Notfällen und anderen schädigenden Ereignissen seine Anwendung finden.
254 „Wenn jede Sekunde zählt“ URL: http://www.as-institute.at/index.php?id=7220 [22.12.2011].
255 Vgl. Bundesministerium für Inneres , 2010, S. 9.
256 „FAQ Allgemein“ URL: http://www.staedtebund.gv.at/services/faq/allgemein.html#c2115 [18.12.2011].
257 Bundesministerium für Inneres , 2010, S. 89.
258 Bundesministerium für Inneres , 2009, S. 11.

Das Subsidiaritätsprinzip führt auch dazu, dass es neun unterschiedliche Katastrophenschutzgesetze – jedes Bundesland hat sein eigenes Gesetz und seine eigenen Begrifflichkeiten – gibt.

5.3 Organisatorische Rahmenbedingungen

Der österreichische Katastrophenschutz baut auf die fünf Säulen

- Bevölkerung,
- Einsatzorganisationen,
- Behörden,
- Wirtschaft und Wissenschaft und
- Forschung

auf. Wobei die letzten beiden Säulen noch relativ jung sind.

Da es in Österreich keine eigenen Organisationen für den Katastrophenschutz gibt, werden diese Aufgaben weitgehend durch Freiwilligenorganisationen, wie den Freiwilligen Feuerwehren oder Rettungsorganisationen, getragen.[259]

> *„Österreich verfügt über mehr als 4.800 Feuerwehren (davon etwa 4.500 Freiwillige Feuerwehren) und über 900 Rettungsstützpunkte. Insgesamt stehen rund 250.000 Aktive bei den Feuerwehren und über 40.000 ausgebildete Sanitäter zur Verfügung.“*[260]

Reichen die Ressourcen der Freiwilligenorganisationen nicht mehr aus, dann kann auch das österreichische Bundesheer im Zuge eines Assistenzeinsatzes gem. § 2. (1) c) des Wehrgesetzes – „die Hilfeleistung bei Elementarereignissen und Unglücksfällen außergewöhnlichen Umfanges“[261] – durch den jeweiligen Einsatz- bzw. Behördenleiter zur Unterstützung angefordert werden.

Im generellen hält sich der Staat Österreich weitgehend aus der Krisenprävention und Krisenreaktion heraus. Bisherige Bestrebungen, wie etwa im Rahmen der Umfassenden Sicherheitsvorsorge (USV) oder dem nationalen Programm zum Schutz kritischer Infrastrukturen (APCIP)[262], eine aktivere Rolle einzunehmen, sind bisher eher auf Sparflamme verlaufen bzw. öffentlich so gut wie nicht wahrzunehmen.

5.3.1 Katastrophenschutzmanagement den Ländern

Im Wesentlichen obliegt das Katastrophenschutzmanagement den Ländern. Hierfür hat jedes Bundesland ein eigenes Katastrophenhilfsgesetz.[263] Dabei werden zwei Bereiche unterschieden (siehe auch Abbildung 7):[264]

259 Vgl. Bundesministerium für Inneres , 2010, S. 30ff.

260 „Aus dem Inneren – Staatliches Krisen- und Katastrophenschutzmanagement“ URL: http://www.bmi.gv.at/cms/bmi/_news/bmi.aspx?id=7A5869735A6A654D596A493D&page=0&view=1 [22.12.2011].

261 „Wehrgesetz 2001“ URL: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001612 [01.01.2012].

262 URL: http://www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf [18.12.2011].

263 Die Gesetze werden unterschiedlich bezeichnet als Katastrophenhilfegesetze, Katastrophenschutzgesetze, Katastrophenmanagementgesetz (Tirol), Krisenmanagementgesetz (Wien).

264 Bundesministerium für Inneres , 2011, S. 24.

- **Katastrophenschutz** (Einsatzvorbereitung, vorbereitende Maßnahmen, Katastrophenschutzplanung, u. a.), entspricht der Phase „Vorsorge“ im Vier-Phasen-Modell;
- **Katastrophenhilfe** (Katastrophenabwehr und -bekämpfung: Intervention, Nachbereitung, Abrechnung, u. a.), entspricht der Phase „Bewältigung“ im Vier-Phasen-Modell.

Neben den Katastrophenhilfsgesetzen gibt es noch zahlreiche andere rechtliche Grundlagen für das Katastrophenschutzmanagement.

> *„Die Einsatzvorbereitung der Katastrophenhilfsdienste der Länder (Feuerwehren, Rettungsorganisationen, ...) ist hingegen nicht in den Katastrophenhilfegesetzen, sondern in anderen Landesgesetzen und -verordnungen (Feuerpolizeigesetze, Mindestausrüstungsverordnungen der Feuerwehren, Rettungsdienstverordnungen) und sonstigen Regelwerken (Richtlinien der Landesregierungen, Richtlinien und Vorschriften der Katastrophenhilfsdienste) geregelt.“*[265]

Zumindest in einigen Bundesländern wird das Thema Blackout seit mehreren Jahren bearbeitet. Hier sind insbesondere Wien und Niederösterreich zu nennen, wo konkrete Bearbeitungen bekannt sind.

5.3.2 Einsatz- und Krisenkoordinationscenter, Bundeswarnzentrale

Seit 2006 steht das Einsatz- und Krisenkoordinationscenter (EKC) mit inkludierter Bundeswarnzentrale (BWZ) beim BM.I zur Verfügung. Es dient als operationelles Koordinations- und Informationsinstrument. Es stellt für diese Angelegenheiten einen nationalen und internationalen Point of Contact (PoC) dar.[266]

Im EKC steht auch ein Call Center zur Verfügung, das jederzeit aktiviert werden kann.

Im EKC ist auch die Bundeswarnzentrale eingebunden. Sie dient als permanente (24/7), österreichische Kontaktstelle, insbesondere für Zwischenfälle in Atomkraftwerken und bei möglicherweise grenzüberschreitenden Katastrophenereignissen. Darüber hinaus dient sie als operationelles Koordinations- und Informationsinstrument für den Zivil- und Katastrophenschutz und für die internationale Katastrophenhilfe. Sie ist auch die Zentralstelle für das gemeinsame Warn- und Alarmsystem des Bundes und der Länder (zentrale Sirenensteuerung, Ringleitung).[267]

5.4 Selbstschutz

Das staatliche Krisen- und Katastrophenschutzmanagement sieht im Selbstschutz der Bevölkerung durch Eigenvorsorge und -bevorratung einen sehr wesentlichen Beitrag zur Vermeidung von Erst- und Folgeschäden.

Besonders wird unterstrichen:

> *„Ein wesentliches Element des Selbstschutzkonzeptes ist auch, dass durch Wissen um Gefahren durch vorhergehende Information im Anlassfall Panik vermieden*

265 Bundesministerium für Inneres , 2011, S. 26.
266 Vgl. „Zivilschutz in Österreich“ URL: http://www.bmi.gv.at/cms/BMI_Zivilschutz/mehr_zum_thema/SKKM.aspx [20.12.2011].
267 Vgl. Bundesministerium für Inneres, 2011, S. 41f.

werden kann. Wirksamer Selbstschutz muss daher auf einer effizienten Risikokommunikation aufbauen.“[268]

„Eine effektive Krisen- und Katastrophenbewältigung ist im hohen Maße von den Fähigkeiten der vor Ort agierenden Hilfs- und Rettungsorganisationen sowie den raschen Lenkungs- und Organisationsmaßnahmen der zuständigen Behörden abhängig. Neben dieser organisierten Hilfe kommt bei Großschadenslagen aber auch der Mitarbeit der betroffenen Bevölkerung eine ganz entscheidende Bedeutung zu. Nur wenn die Bevölkerung über das richtige Verhalten in Notsituationen informiert ist und die richtigen Sofortmaßnahmen zum eigenen Schutz und zum Schutz der Nachbarschaft setzten kann, bleibt den Einsatzkräften jener Zeitraum, den sie zur Bewältigung von Katastrophenlagen benötigen.“[269]

5.4.1 Information durch das BM.I

Das BMI bildet auf der Homepage www.bmi.gv.at/zivilschutz „zentrale Themenbereiche des Zivilschutzes, nämlich den Brand-, Strahlen- und Störfallschutz ab.“[270]

5.4.2 Information durch den Österreichischen Zivilschutzverband

Der Österreichische Zivilschutzverband (ÖZSV) ist der „verlängerter Arm des BM.I“, welcher Zivil- und Selbstschutzinformationen durch Herausgabe von Broschüren, Zeitschriften, Plakaten und durch Abhalten von Vorträgen und Veranstaltungen an die Bevölkerung weitergibt.

Darüber hinaus werden die Sicherheits-Informationszentren (SIZ) auf Gemeindeebene betrieben. Mit Hilfe dieser Informations- und Beratungsstellen in den Gemeinden soll vor allem die Bevölkerung über die zentralen Themen (Brandschutz, Erste Hilfe, Strahlenschutz, Warnung und Alarmierung, Bevorratung und Kriminalitätsvorbeugung) des Selbstschutzes informiert werden.[271]

5.5 Zusammenfassung

Wie wahrscheinlich bei der Lektüre dieses Kapitels aufgefallen ist, gibt es mehrere Hinweise, dass das derzeitige nationale Krisen- und Katastrophenschutzmanagement wahrscheinlich bei einem Blackout nur bedingt handlungsfähig sein wird. Im Zuge von Kontaktaufnahmen zu den entsprechenden Einrichtungen wurde dieser Eindruck noch erheblich verstärkt. Einerseits wird für dieses Thema keine Zuständigkeit angenommen und auf der anderen Seite wird die Möglichkeit eines Blackouts „aufgrund der sehr guten Infrastruktur“ de-facto ausgeschlossen und kein Handlungsbedarf gesehen. Daher gibt es auch keine generelle Information der Bevölkerung und das Thema Blackout wird auf den entsprechenden Informationsseiten nicht abgebildet.[272]

Dies stellt einen ganz klaren Widerspruch zu den Aussagen zum Selbstschutz der Bevölkerung dar,[273] was sich auch immer wieder im Rahmen von persönlichen Gesprächen

268 Bundesministerium für Inneres , 2010, S. 104.
269 Bundesministerium für Inneres , 2011, S. 52.
270 ebenda, S. 53.
271 ebenda, S. 54.
272 Vgl. Abschnitt 5.4.1, Information durch das BM.I, und Abschnitt 5.4.2, Information durch den Österreichischen Zivilschutzverband.
273 Vgl. Abschnitt 5.4, Selbstschutz.

bestätigte. Ein tiefer gehendes Gespräch zum Thema Blackout führte bei den meisten Personen zu großer Betroffenheit, aber auch zur Bereitschaft selbst zu handeln. Dies spiegelt sich auch in einer aktuellen Umfrage wieder, wo festgestellt wird, dass Krisenprävention und Risikomanagement in Österreich nur eine geringe Bedeutung haben. Zwei Drittel aller Befragten glauben, dass die österreichischen Behörden im Vergleich zu anderen Ländern schlechter auf Krisen vorbereitet sind.[274]

> *„Neben der Abhängigkeit von Infrastrukturen und Informationstechnologie stellen demnach auch die abnehmende Selbsthilfefähigkeit und das geringe Risikobewusstsein der Bevölkerung Risikofaktoren dar."*[275]

Daher muss festgehalten werden, dass die derzeit fehlende Risikokommunikation und Eigenvorsorge, bei einem Eintritt eines Blackouts, massive negative Auswirkungen auf die Bewältigung haben wird.

> *„Eine ausgeprägte Selbstverantwortung trägt dazu bei, sowohl die Eintrittswahrscheinlichkeit als auch die Schwere von Katastrophen zu mindern."*[276]

Ein weiterer massiver Schwachpunkt ist die sehr starke föderale Ausrichtung Österreichs und das Subsidiaritätsprinzip, wodurch es weitgehend an einer operativen gesamtstaatlichen Koordinierungsfähigkeit fehlt, welche bei einem Blackout zwingend erforderlich wäre. Erschwerend kommt hinzu, dass im jeweiligen Bundesland unterschiedliche Begriffe und Rechtsgrundlagen zur Anwendung kommen. Eine ländergrenzenüberschreitende Zusammenarbeit wird dadurch erheblich erschwert bzw. kostet großen Koordinierungsaufwand. Es gibt zwar einen Koordinierungsausschuss, der aber wahrscheinlich bei einem Blackout nicht mehr operativ tätig werden kann. Die Zusammenarbeit beruht auf Freiwilligkeit.

> *„Die Verantwortung für den Katastrophenschutz wird auf sehr viele Funktionen verteilt. Daraus erwachsen zum einen viele Chancen wie Flexibilität, Wettbewerb, Sicherheit durch Redundanzen und Möglichkeit der Selbstregulierung. Zum anderen entstehen auch Risiken wie unklare Zuständigkeiten, Organisationslücken, Doppelarbeiten, sehr komplizierte Koordination und Steuerung und fehlende einheitliche Kontrolle."*[277]

Grundsätzlich soll die Katastrophenhilfe auch weiterhin möglichst weit unten an der Basis erfolgen und den Bundesländern keine Kompetenz weg genommen werden. Ein derart zeitkritisches Ereignis wie ein Blackout erfordert aber bereits im Vorfeld erheblichen Koordinierungsaufwand, der nicht nur auf freiwilliger Basis erfolgen kann, da das Gesamtsystem – das Gemeinwohl aller Bürger – davon abhängt.

Natürlich kann die Frage der Wahrscheinlichkeit eines Eintritts gestellt werden. Hierzu ist auf den Abschnitt 1.2.11, Restrisiko, zu verweisen. Gleichzeit muss einmal mehr die aktuelle Terrorgefahr für Österreich hinterfragt werden, wenn sie sogar im Zivilschutz

274 Vgl. „Österreichs Unternehmen sind auf Krisen schlecht vorbereitet" URL: http://www.pressetext.com/news/20110916015 [01.01.2012].

275 „Hilfe in der Not" URL: http://www.sicherheit.info/si/cms.nsf/si.ArticlesByDocID/1102810?Open [01.01.2012].

276 „Katastrophenschutz geht alle an" URL: https://www.allianzdeutschland.de/news/news-2008/26-11-08-katastrophenschutz-geht-alle-an [21.12.2011].

277 Allianz Deutschland AG, 2008, S. 4.

als dezidiertes Beispiel – „Vorsorgen zum Schutz vor möglichen Auswirkungen des internationalen Terrorismus.“[278] – angeführt wird.

5.5.1 SKKM-Strategie 2020

Im Juli 2009 wurde die „SKKM-Strategie 2020“ durch den Ministerrat genehmigt. In dieser sind einige, auch für das Szenario Blackout, relevante Punkte zu finden. Eine entsprechende Umsetzung sollte daher möglichst zeitnah erfolgen.

> *„Die Bevölkerung wird in das Krisen und Katastrophenschutzmanagement durch die Förderung des Selbstschutzgedankens und laufende Informations- und Aufklärungsarbeit der Behörden sowie des Österreichischen Zivilschutzverbandes einbezogen. (…)*
>
> *Die im Bundesstaat erforderliche Kooperation und Koordination wird durch das beim BM.I angesiedelte SKKM sowohl in der Grundsatzplanung wie im Anlassfall gewährleistet.“*[279]
>
> *„(...) bestmögliche Verhinderung von Katastrophen durch Prävention und Risikooptimierung (…) Umsetzung technischer Innovationen, insbesondere zur Verbesserung des Informationsflusses zu den bzw. zwischen strategischen Entscheidungsträgern und zur Verbesserung der anlassfallbezogenen Kommunikation mit der Bevölkerung; “*[280]
>
> *„In der effizienten Warnung der Bevölkerung bzw. in der Risikokommunikation wird vielfach eine bestehende Lücke im System des Bevölkerungsschutzes gesehen.“*[281]
>
> *„Darüber hinaus sollte auch eine regelmäßige Beübung der strategischen Ebene des SKKM (Koordinationsausschuss) im Hinblick auf längerfristige Entscheidungsprozesse in Krisensituationen etabliert werden.“*[282]
>
> *„Eine zusätzliche Herausforderung stellt in dem Zusammenhang die Kompetenzzersplitterung in der österreichischen Bundesverfassung dar.“*[283]

Der Bezug zum Thema Blackout ist mit einem Satz angeführt:

> *„Ausfall kritischer Infrastrukturen, wobei hierbei vordergründig das Szenario eines längeren Stromausfalles und aller seiner sekundären Folgeerscheinungen zu betrachten ist.“*[284]

Ob diese Intentionen mit den bereits in der Strategie angeführten Selbstbeschränkungen zu erreichen sein werden, wird die Zukunft zeigen:

> *„Risikoanalysen sind aber immer nur so weit von tatsächlichem Nutzen bzw. ist der Aufwand für deren Erstellung nur soweit tatsächlich gerechtfertigt, als sie Systementscheidungen (z. B. Legistik, Investitionsprogramme) tatsächlich beein-*

278 „Zivilschutz in Österreich“ URL: http://www.bmi.gv.at/cms/BMI_Zivilschutz/ [01.01.2012].
279 Bundesministerium für Inneres, 2009, S. 6.
280 ebenda, S. 7.
281 ebenda, S. 9.
282 ebenda, S. 11.
283 ebenda, S. 12.
284 ebenda, S. 7.

flussen können. Realistisch betrachtet hängen Systementscheidungen auch nicht allein von objektiven Risikofaktoren ab, sondern auch von anderen gesellschaftlichen Einflussfaktoren und finanziellen Schranken, was den Nutzen von gesamtstaatlichen Risikoanalysen wiederum schmälert."[285]

„Eine gesamtösterreichische Steuerung des Mitteleinsatzes für den Katastrophenschutz ist infolge der überwiegenden Zuständigkeit der Bundesländer und des Ressortprinzips grundsätzlich nicht möglich."[286]

Die Herausforderungen aufgrund der derzeitigen Realpolitik und der Notwendigkeit einer Anpassung der Verfassung, um die Kompetenzlage im Katastrophenschutzmanagement neu zu regeln, sind natürlich enorm.[287]

Das Fehlen einer eigenen Zivil-/Bevölkerungsschutzbehörde wirkt sich auf vielen Ebenen nachteilig aus. Dies betrifft nicht nur den Risikokommunikations- oder Koordinierungsbereich, sondern bereits die Risikoerfassung.

„Forschungsaktivitäten im Bereich des Krisen- und Katastrophenschutzmanagements werden derzeit in Österreich nicht systematisch erfasst. (…) Der Zugang der Entscheidungsträger im SKKM zu Ergebnissen ist jedoch schwierig und derzeit kaum zu bewerkstelligen. (…) Zentralstellen für das Katastrophenmanagement in anderen Staaten nehmen den Bereich der Forschung vergleichsweise systematisch wahr, indem sie eigene Forschungsdokumentationen aufbauen und selbst gezielt Forschungsaufträge vergeben."[288]

Zusammengefasst kann festgehalten werden, dass es in der SKKM-Strategie 2020 einige Anhaltspunkte zur Verbesserung des österreichischen Krisen- und Katastrophenschutzmanagements, auch hinsichtlich der Anpassung an neue Herausforderungen, gibt. Aufgrund der aber bereits in der Strategie festgehaltenen Selbstzweifel hinsichtlich einer Umsetzbarkeit muss befürchtet werden, dass auch hier der österreichische Weg gegangen wird. So lange nichts passiert, wird es auch keine entsprechenden Anstrengungen geben. Eine Vorgangsweise, die insbesondere beim Thema Blackout unverantwortlich ist.

„Es gibt zwei Dinge, die vermisst man, wenn man sie verloren hat:
Sicherheit und Gesundheit."

Thomas Müller

285 Bundesministerium für Inneres, 2009, S. 15.
286 ebenda, S. 21.
287 Vgl. Bundesministerium für Inneres, 2009, S. 12.
288 Bundesministerium für Inneres, 2009, S. 20.

6 Schlussfolgerungen

Bereits nach dem Kapitel Krisen- und Katastrophenereignisse war zu erwarten, dass das Know-how für generell erforderliche Krisenpräventions- und Krisenreaktionsmaßnahmen nicht neu entwickelt werden muss, sondern die dazu erforderlichen Erkenntnisse bereits vielfach vorliegen. Dennoch entstand im Rahmen der Analyse der Eindruck, dass auch in gesellschaftlich hoch kritischen Bereichen nicht „aus der Geschichte" gelernt wird und diese anscheinend immer wieder wiederholt werden muss. Großschäden und Katastrophen entstehen nie aufgrund einzelner Ursachen sondern basieren immer auf mehreren Einflussfaktoren, die für sich alleine harmlos sind. Diese können bereits vorher lange vorhanden und auch bekannt sein. In der Regel gibt es zwischen diesen Einflussfaktoren oder Katastrophenauslösern auch keine Verknüpfungen. Erst die unvorhergesehene Verknüpfung, die durch seltene Zufälle oder bei unüberlegten Systemeingriffen erfolgt, wird ein negativer Dominoeffekt ausgelöst.[289] [290] [291] Positiv gesehen heißt das, dass die vorhandenen Erkenntnisse nur zusammengeführt, analysiert und für den jeweiligen Bedarf angepasst werden müssen.

Im Rahmen der Analyse des österreichischen Krisen- und Katastrophenschutzmanagements im Kapitel Der Zivilschutz in Österreich hat sich eine Hypothese ergeben, die im Rahmen der folgenden Masterarbeit zu verifizieren ist. Sie stellt in den Raum, dass das derzeitige österreichische Krisen- und Katastrophenschutzmanagement nicht ausreichend auf überregionale und zeitkritische Krisenereignisse, wie etwa ein Blackout oder einen größeren Angriff auf bzw. den Ausfall von IKT, vorbereitet ist, und dass dies schwerwiegende negative Konsequenzen für die Bewältigung erwarten lässt. Diese Annahme gilt natürlich nicht pauschal. So muss festgehalten werden, dass z. B. auf Landesebene sehr wohl Vorkehrungen und Überlegungen bzgl. der Bewältigung eines möglichen Blackouts laufen, wenngleich eine tiefer gehende Analyse im Rahmen dieser Arbeit nicht möglich war.

Eine mögliche Ursache dafür könnte in der mangelnden Auseinandersetzung mit komplexen Systemen, wie im Kapitel Komplexe Systeme und die Stromversorgung erläutert, zu finden sein. Auch diese Annahme muss in weiterer Folge weiter verifiziert werden.

Wesentliches Ziel dieser Analyse ist es, mögliche Systemzusammenhänge aufzuzeigen und Gedankenanstöße zu liefern. Sie soll vor allem den verantwortlichen Stellen im Bereich des Krisen- und Katastrophenschutzmanagements als Unterstützung und Argumentationshilfe dienen. Nicht-Ziel ist eine „Panikmacherei" oder die Beschreibung eines „Weltuntergangsszenarios", was in jedem Fall kontraproduktiv wäre. Es muss aber allen bewusst werden, dass die globale Vernetzung nicht nur ihre positiven Seiten hat. Daher müssen wir unsere Fähigkeiten zur Bewältigung von möglichen negativen Auswirkungen verstärkt an die neuen Gegebenheiten anpassen. Wir müssen unsere Krisen- und Katastrophenschutzmaßnahmen laufend weiterentwickeln und vor allem der Geschwindigkeit der sonstigen Entwicklungen anpassen. Zeithorizonte von mehr als 5 Jahren dürften dabei wenig realistisch sein. Andernfalls provozieren wir unfreiwillig neue Krisen und Ka-

289 Vgl. Kapitel Krisen- und Katastrophenereignisse.

290 Vgl. Allianz Deutschland AG, 2008, S. 17.

291 Als Negativbeispiel muss einmal mehr die, in der derzeitigen Form, beabsichtigte Einführung von intelligenten Stromzählern angeführt werden. Vgl. Saurugg, 2011b.

tastrophen. Daher ist es erforderlich, dass wir unser Hauptaugenmerk auf die Entwicklung eines adäquaten Risiko- und Chancenbewusstseins, sowie auf erforderliche Organisationsentwicklungen und vor allem auf den Selbstschutz und die Selbsthilfefähigkeit der Bevölkerung richten.[292]

Es müssen dabei sicher auch schmale Grade betreten werden.

> *„Eine permanente Informationsflut zum Thema Schutzmechanismen würde bewirken, dass zunächst Unruhe entstehen würde. Der Bürger wird verunsichert. Kommt es dann nicht zu der erwarteten Schadenslage, setzt ein Desinteresse ein."*[293]

Abschließend sollen die eingangs gestellten Forschungsfragen beantwortet werden. Auf eine erforderliche Detaillierung muss hier aufgrund des Umfanges verzichtet werden, welche jedoch in der Masterarbeit erfolgen wird.

6.1 Sind Blackouts eine reale Bedrohung oder reine „Angstmacherei"?

Aufgrund der in der jüngsten Vergangenheit erfolgten und im Kapitel Stromversorgungssicherheit aufgezeigten massiven Eingriffe in das hochkomplexe System der europäischen Stromversorgung, muss diese Frage mit einem eindeutigen Ja – Blackouts sind eine reale Bedrohung – beantwortet werden.

Der deutsche, überparteiliche Verein, Zukunftsforum öffentliche Sicherheit e.V., hat bereits 2008 die unmittelbare Eintrittswahrscheinlichkeit von Blackouts in Deutschland mit hoch eingestuft.[294] [295] Aufgrund der tiefgehenden Systemänderungen wäre zu hinterfragen, ob diese Klassifizierung noch Gültigkeit besitzt. Weiters wurde damals festgehalten, dass „ein hohes Risiko für Menschen, Staat und Wirtschaft" besteht.

Nicht beantwortet werden kann hier, in welchem Umfang oder mit welcher Häufigkeit wir damit rechnen müssen. Auch nicht, wann ein solches Ereignis eintreten bzw. wie lange es dauern wird. Dazu gibt es einfach zu viele unbekannte Parameter. Teilblackouts, z. B. durch erforderliche Notabschaltungen ganzer Regionen zur Stabilisierung des restlichen Netzes, sind in jedem Fall bereits angekündigt worden und können bereits in naher Zukunft, noch im Winter 2012, Realität werden.[296]

Es darf davon ausgegangen werden, dass die Netzbetreiber und EVUs alles daran setzen werden, Blackouts zu verhindern bzw. so rasch wie möglich zu beheben. Unsere moderne Gesellschaft mit ihrem sehr stromabhängigen Lebensstil ist jedoch gut beraten, sich dennoch auf solche Ereignisse vorzubereiten. Bei Eintritt eines solchen weitreichenden Stromausfalles wird es dazu kaum mehr Möglichkeiten geben. Darüber hinaus handelt es sich um ein sehr zeitkritisches Ereignis.

292 Allianz Deutschland AG, 2008, S. 49.
293 Fachhochschule Münster, 2006, S. 31.
294 Vgl. Zukunftsforum öffentliche Sicherheit, 2008, S. 19.
295 Einstufung: vgl. Abschnitt 1.2.9, Risiko und Risikomanagement.
296 Vgl. „Rede vor dem RWE-Beirat " URL: http://www.rwe.com/web/cms/mediablob/de/718044/data/213092/2/rwe/investor-relations/events-praesentationen/archiv/07.07.2011.pdf [04.01.2012].

Durch den Umfang der Betroffenheit – so gut wie niemand wird davon verschont bleiben, da fast unsere gesamte, überlebensnotwendige Infrastruktur involviert wird – handelt es sich um ein einzigartiges Schlüsselszenario.

6.2 Ist das nationale Krisen- und Katastrophenschutzmanagement ausreichend auf ein solches Szenario vorbereitet?

Wie im Kapitel Der Zivilschutz in Österreich erläutert wurde, muss davon ausgegangen werden, dass das nationale Krisen- und Katastrophenschutzmanagement derzeit nicht ausreichend auf ein derartiges Szenario vorbereitet ist.

Die größte Schwachstelle ist dabei wohl in der mangelnden Information und Sensibilisierung der Bevölkerung und der damit ursächlich zusammenhängenden, wohl weitgehend fehlenden, Eigenvorsorge zu sehen. Diese wird sich vor allem in Ballungsräumen massiv negativ auf die Bewältigung eines solchen Schlüsselszenarios auswirken, insbesondere, wenn die Behebung länger als ein paar Stunden andauert, von dem ausgegangen werden muss.

Eine Besonderheit bei einem Blackout ist, dass die BOS und Katastrophenschutz- und -hilfsorganisationen nicht mehr primär Retter, sondern ebenfalls Opfer sind und daher die Standardverfahren nicht ausreichen werden.

6.3 Besteht Handlungsbedarf? Wenn ja, in welchen Bereichen?

Es besteht absoluter Handlungsbedarf.

Hier darf auch noch besonders auf die Zusammenfassungen des Kapitels Krisen- und Katastrophenereignisse ab Seite 28 und des Kapitels Der Zivilschutz in Österreich ab Seite 61 verwiesen werden.

6.3.1 Risikobewusstsein und Risikokommunikation, Krisenkommunikation

Das fehlende Risikobewusstsein beginnt damit, dass anscheinend die verantwortlichen Stellen sich der vollen Tragweite nicht bewusst sind oder nicht ausreichend Gehör finden. Dass dies in Zeiten der Finanz- und sonstigen Krisen nicht immer einfach ist, ist durchaus nachvollziehbar, aber im Anlassfall nicht entschuldbar. Darüber hinaus muss klar sein, dass bei einem Eintritt und den damit zu erwartenden finanziellen Schäden – bis zu 900 Millionen Euro pro Tag[297] – eine Euro- oder Staatsschuldenkrise wahrscheinlich völlig eskaliert und nicht mehr beherrschbar sein wird. Ganz abgesehen von den sonstigen Folgeschäden für den Wirtschaftsstandort Österreich. Im Sinne des Kapitels Komplexe Systeme und die Stromversorgung sollten derartige Zusammenhänge in aktuelle Lagebeurteilungen einfließen und als systemrelevante Variablen gesehen werden.

Bei der Risikoerfassung und Auswertung ist darauf zu achten, dass man sich nicht durch die möglichen Risiken paralysieren lässt, sondern vor allem auf die Chancen für neue Entwicklungsmöglichkeiten achtet.

> *„Risiken erfordern zunächst den Umgang mit Veränderungen jeder Art, insbesondere aber den Umgang mit extrem schnellen, mit unerwarteten oder hochdyna-*

297 Vgl. Abschnitt 4.1, Blackout.

mischen Veränderungen, die sich unserer Kontrolle mehr oder weniger vollständig entziehen."[298]

Die etwas sarkastische Aussage, jede Krise hat auch ihre Chancen, hat durchaus einen wahren Kern. Wenn sich herausstellt, dass ein System aufgrund der Komplexität offensichtlich nicht mehr beherrschbar ist, dann müssen im Sinne der Kybernetik[299] neue Wege und Lösungen gesucht werden, die diese Beherrschbarkeit wieder gewährleisten. Nur so kann eine langfristige Überlebensfähigkeit des Systems geschaffen werden.[300]

„Stabilität oder – wie die Biologen es nennen – Robustheit setzen sich in der Evolution eher durch als Nützlichkeit. Nutzen ist aber das Kriterium der Wirtschaft und damit in unserer Gesellschaft heute das schärfste Schwert in der Argumentation."[301]

Ein wesentlicher Beitrag zu einer Risikoabschätzung wird durch eine entsprechende Technikfolgenabschätzung geliefert, welche durch eine unabhängige Organisation durchzuführen ist.[302] Dabei sollte berücksichtigt werden, dass „Phantasie wichtiger als Wissen ist, da Wissen begrenzt ist".[303]

Das Ziel einer Risikokommunikation muss es sein, das Bewusstsein für Risiken zu schaffen und zu vermitteln, wer welchen Beitrag zur einer möglichen Bewältigung liefern kann bzw. muss. Besonders Wert ist dabei auf die Förderung der Eigenverantwortung zu legen. Denn ganz wesentlich ist, dass jeder Einzelne mit seinem Verhalten einen positiven oder negativen Beitrag zum Verlauf einer Krise beisteuert. Die Bekanntheit einer Bedrohung und der dazu erforderlichen Verhaltens- und Bewältigungsmaßnahmen verhindern einen Überraschungseffekt und die daraus entstehende Hilflosigkeit.

Im Krisenfall wird die Risikokommunikation zur Krisenkommunikation. Diese bestimmt wesentlich

„(...) die Durchhaltefähigkeit der Bevölkerung, die Akzeptanz des Krisenmanagements und die Frage, wie sozial oder unsozial die Menschen in der Krise reagieren. Dazu gehören verlässliche, keinesfalls beschönigende Informationen und die Einbindung der Bevölkerung als aktiver Akteur."[304]

Eine Krisenkommunikation erfordert eine professionelle Vorbereitung.

6.3.2 Selbsthilfefähigkeit der Bevölkerung

Die Selbsthilfefähigkeit der Bevölkerung, der Selbstschutz sowie Selbst- und Nachbarschaftshilfe, müssen deutlich gesteigert werden. Dazu ist eine entsprechende Risikokommunikation und Sensibilisierung erforderlich, welche nicht einfach sein wird. Sie stellt einen Widerspruch zur derzeitigen Mentalität einer „Vollkasko-Gesellschaft" und

298 Witzer, 2011, S. 172.
299 Vgl. Kapitel Komplexe Systeme und die Stromversorgung.
300 Vgl. Allianz Deutschland AG, 2008, S. 6.
301 Witzer, 2011, S. 173.
302 Vgl. Abschnitt 3.6.5 Technikfolgenabschätzung – Sicherheitsvorschriften und Kontrolle.
303 Vgl. Witzer, 2011, S. 244.
304 Forschungsforum Öffentliche Sicherheit, 2010b, S. 2.

„irgendwer ist schon zuständig oder wird das bezahlen“ dar. Wer das bezahlen wird, steht bereits fest – die Steuerzahler. Eine mögliche Krisenkommunikation wird aber um Dimensionen schwieriger ausfallen. Die gesellschaftspolitischen Auswirkungen sind dabei nicht absehbar. Es wird aber wahrscheinlich danach kein „vor der Krise“ geben. Eine wesentliche Hürde ist, dass Menschen immer Vergleiche zu erlebten Ereignissen ziehen und kaum den Bezug zu nicht erlebten Ereignissen herstellen können.

> *„Dabei ist die Selbsthilfefähigkeit bei der Frage entscheidend, wie viel Zeit zwischen dem Beginn der Katastrophe und der irreversiblen Zerstörung sozialer Strukturen vergeht.“*[305]

6.3.3 Organisatorische Rahmenbedingungen

Wie bereits mehrfach angeführt wurde, scheint eine Anpassung der organisatorischen Rahmenbedingungen für das nationale Krisen- und Katastrophenschutzmanagement, insbesondere für hoch zeitkritische und überregionale Ereignisse, zwingend geboten. Eine weitere Bearbeitung erfolgt in der Masterarbeit.

6.3.4 Medien

Eine ganz wesentliche Rolle bei der Risiko- und Krisenkommunikation spielen die Medien. Bei einer nichtprofessionellen Informationspolitik kann sehr viel Schaden auf verschiedenen Ebenen verursacht werden. Auf der anderen Seite ist bei einer entsprechenden Vorgehensweise und Vertrauensbasis ein sehr positives und konstruktives Zusammenwirken möglich und auch zwingend erforderlich. Als Grundlage könnte die Medienarbeit im Fall eines Suizides herangezogen werden. Hier gibt es eine generelle Selbstbeschränkung durch die Medien, da nachgewiesen ist, dass eine entsprechende Berichterstattung zu Nachahmungstaten führt.

6.3.5 Internationale Zusammenarbeit

Im Vergleich Österreich / Deutschland gibt es sehr viele Parallelen, etwa in den Strukturen der Katastrophenhilfe, aber auch bei den möglichen Ereignissen und Folgen. Daher erscheint es angebracht, mangels eigener Kapazitäten und Analysen diese Erkenntnisse intensiver für konkrete, eigene Ableitungen zu nutzen. Gerade für derart komplexe Szenarien, die hoch zeitkritisch und meist überregional vernetzt und abhängig sind, erscheint es zielführend, die internationale Zusammenarbeit insbesondere im D-A-CH[306] Bereich zu forcieren. Eine internationale Zusammenarbeit zur Bewältigung derartiger Krisen wird in jedem Fall erforderlich sein.

„Krise kann ein produktiver Zustand sein.
Man muss ihr nur den Beigeschmack der Katastrophe nehmen.“
(Max Frisch)

305 Forschungsforum Öffentliche Sicherheit, 2010b, S. 2.

306 Deutschland – Austria (Österreich) – Confoederatio Helvetica (Schweiz)

7 Literaturverzeichnis

Allianz Deutschland AG (Hrsg.): *Katastrophenschutz auf dem Prüfstand/Analysen, Prognosen und Empfehlungen für Deutschland.* In: Internet, 2008, unter URL: http://www.dgkm.org/pdf.php?id=1190&lang=de&name=Katastrophenschutz+auf+dem+Pr%C3%BCfstand+-+Studie+der+Allianz+AG [21.12.2011]

Beck, Ulrich: *Risikogesellschaft/Auf dem Weg in eine andere Moderne.* Berlin: Suhrkamp 1986

Bundeskanzleramt (Hrsg.): *Das österreichische Programm zum Schutz kritischer Infrastrukturen, Masterplan APCIP.* Wien: BKA, 2008, unter URL: http://www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf [02.12.2011]

Bundesministerium des Innern (Hrsg.): *Schutz Kritischer Infrastrukturen – Basisschutzkonzept/Empfehlungen für Unternehmen.* Berlin: BMI, 2005, unter URL: http://www.bmi.bund.de/cae/servlet/contentblob/131040/publicationFile/13132/Basisschutzkonzept_kritische_Infrastrukturen.pdf [08.12.2011]

Bundesministerium für Inneres (Hrsg.): *SKKM Strategie 2020.* Wien: BM.I., 2009, unter URL: http://www.sicherheit.ktn.gv.at/171192_DE-.pdf [21.12.2011]

Bundesministerium für Inneres (Hrsg.): *Staatliches Krisen- und Katastrophenschutzmanagement/Rechtliche und organisatorische Grundlagen.* Wien: BM.I., 2010

Bundesministerium für Inneres (Hrsg.): .*SICHERHEITSBERICHT 2010/KRIMINALITÄT 2010 VORBEUGUNG UND BEKÄMPFUNG.* Wien: BM.I., 2011, Unter URL: http://www.parlament.gv.at/PAKT/VHG/XXIV/III/III_00273/imfname_231954.pdf [21.12.2011]

Bundesministerium für Inneres (Hrsg.): *Koordination von Krisen- und Katastrophenschutzmanagement/Fachgespräch mit Innenministerin Maria Fekter am 24.03.2011.* Wien: BM.I., 2011, unter URL: http://www.bmi.gv.at/cms/cs03documentsbmi/983.pdf [22.12.2011]

Bundesnetzagentur (Hrsg.): *Bericht über die Systemstörung im deutschen und europäischen Verbundsystem am 4. November 2006.* In: Internet, 2007, unter URL: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Energie/Sonderthemen/Stromausfall4Nov06/BerichtId9007pdf.pdf?__blob=publicationFile [04.12.2011]

Bundesnetzagentur (Hrsg.): *Auswirkungen des Kernkraftwerk-Moratoriums auf die Übertragungsnetze und die Versorgungssicherheit − AKTUALISIERUNG.* In: Internet, 2011, unter URL: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Presse/Berichte/2011/FortschreibungMoratoriumsBericht26Mai2011pdf.pdf?__blob=publicationFile [03.01.2012], (zit. 2011a)

Bundesnetzagentur (Hrsg.): *„Smart Grid" und „Smart Market"/Eckpunktepapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems.*

In: Internet, 2011, unter URL: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Energie/Sonderthemen/SmartGridEckpunktepapier/SmartGridPapierpdf.pdf?__blob=publicationFile [17.01.2012], (zit. 2011b)

Büro für Technikfolgenabschätzung beim Deutschen Bundestag (Hrsg.): *Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung.* In: Internet, 2011, unter URL: http://dipbt.bundestag.de/dip21/btd/17/056/1705672.pdf [04.01.2012]

Centra Technology, Inc.: *OECD/IFP Futures Project on "Future Global Shocks"/"Geomagnetic Storms".* In: Internet, 2011, unter URL: http://www.oecd.org/dataoecd/57/25/46891645.pdf [16.12.2011]

CRO Forum (Hrsg.): *Power Blackout Risks/Risk Management Options/Emerging Risk Initiative – Position Paper.* In: Internet, 2011, unter URL: http://www.thecroforum.org/assets/files/publications/CRO-Position%20Paper%20-%20Power%20Blackout%20Risks-.pdf [12.12.2011]

Dorn, Jochen: *Organisationen als komplexe Systeme/Interventionsund Entwicklungsmöglichkeiten.* In: Internet, 2004, unter URL: http://www.jochendorn.de/mediapool/28/285746/data/Organisationen%20als%20komplexe%20Systeme.pdf [17.12.2011]

Dörner, Dietrich: *Die Logik des Mislingens/Strategisches Denken in komplexen Situationen.* Hamburg, 2011[10]

Energietechnische Gesellschaft im VDE (Hrsg.): *Stromversorgungsstörungen in den USA/Kanadam, London, Schweden/Dänemark und Italien/Anlässe und Abläufe Ursachen und Konsequenzen.* In: Internet, 2003, unter URL: http://www.vde.com/de/fg/ETG/Pbl/Studien/Documents/MCMS/Blackoutbericht6.pdf [31.10.2011]

ENISA (Hrsg.): *National Risk Management Preparedness.* In: Internet, 2011, unter URL: http://www.enisa.europa.eu/act/rm/files/deliverables/WG%202010%20NRMP [04.01.2012]

Fachhochschule Münster (Hrsg.): *Auswirkungen des Ausfalls Kritischer Infrastrukturen auf den Ernährungssektor am Beispiel des Stromausfalls im Münsterland im Herbst 2005*. In: Internet, 2008, unter URL: http://www.hb.fh-muenster.de/opus/fhms/volltexte/2011/677/pdf/Stromausfall_Muensterland.pdf [01.11.2011]

Foerster, Heinz von: *Wahrheit ist die Erfindung eines Lügners/Gespräch für Skeptiker.* Heidelberg: Carl-Auer-Systeme Verlag und Verlagsbuchhandlung GmbH, 2011[9]

Forschungsforum Öffentliche Sicherheit (Hrsg.): *Kritische Infrastrukturen aus Sicht der Bevölkerung.* In: Internet, 2010, unter URL: http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_3.pdf [04.01.2012], (zit. 2010a)

Forschungsforum Öffentliche Sicherheit (Hrsg.): *Kritische Infrastrukturen aus Sicht der Bevölkerung - Kurzfassung.* In: Internet, 2010b, unter URL: http://www.sicherheit-forschung.de/schriftenreihe/sr_kf/sr_3_kf.pdf [04.01.2012], (zit. 2010b)

Freie Universität Berlin (Hrsg.): *Workshop „Biologische Gefahren – Prävention, Reaktion und Wahrnehmung durch die Bevölkerung“/Dokumentation*. In: Internet, 2011, unter URL: http://www.sicherheit-forschung.de/workshops/workshop_4/doku_ws_4/doku_ws_4.pdf [09.12.2011]

Klimaund Energiefonds: *Geförderte Projekte – Smart Grids Zusammenstellung ausgewählter Projekte Aktualisierte Fassung – 2011.* In: Internet, 2011, unter URL: http://www.ffg.at/sites/default/files/allgemeine_downloads/smart_grids_2011.pdf [04.01.2012]

Göllner, Johannes/Kienesberger, Gottfried/Peer, Andreas: *Wissensmanagement im ÖBH/Analyse und Betrachtung von Kritischen Infrastrukturen.* Wien: BMLVS, 2010, (zit. 2011a)

Göllner, Johannes/Meurers, Christian/Peer, Andreas: *Wissensmanagement im ÖBH/Systemdefinition, Systembeschreibung und Systembegrenzung zur Szenarienentwicklung und Szenariomodellierung Teil 1: Allgemeine Systemdefinition und Systembeschreibung.* Wien: BMLVS, 2010, (zit. 2011b)

Göllner, Johannes/Meurers, Christian/Peer, Andreas/Povoden, Günter: *Wissensmanagement im ÖBH/Systemdefinition, Systembeschreibung und Systembegrenzung zur Szenarienentwicklung und Szenariomodellierung Teil 2: Darstellung von ausgewählten Methoden und möglichen Teilsystemen.* Wien: BMLVS, 2010, (zit. 2011c)

Göllner, Johannes/Meurers, Christian/Peer, Andreas/Povoden, Günter: *Wissensmanagement im ÖBH/Systemdefinition, Systembeschreibung und Systembegrenzung zur Szenarienentwicklung und Szenariomodellierung Teil 3A: Einführung in Szenarienentwicklung und Szenariomanagement-Grundlagen, Szenariotechnik und Szenarioplanung.* Wien: BMLVS, 2010, (zit. 2011d)

Koler, Barbara: *Krisenmanagement im Katastrophenfall am Beispiel Tirol Organisation und rechtliche Grundlagen*. Innsbruck: Universität Innsbruck, Diplomarbeit, 2000, unter URL: http://essc.dreamhosters.com/online/fileadmin/Dokumente_-_OEffentliche_Informationssammlung/krisenmanagement-rechtsgrundlagen-bkoler1.pdf [04.01.2012]

Ladinig, Udo: *BLACK OUT/Maßnahmen des Militärkommando NIEDERÖSTERREICH bei BLACK OUT in der Stromversorgung*. Wien: Eigenverlag, 2010

Mainzer, Klaus: *Was sind komplexe Systeme?/Komplexitätsforschung als integrative Wissenschaft.* In: Internet, 2004, unter URL: http://www.integrative-wissenschaft.de/Archiv/dokumente/Mainzer-14_10_04.pdf [16.01.2012]

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (Hrsg): *Deep Water/The Gulf Oil Disaster and the Future Report to the President.* In: Internet, 2011, unter URL: http://www.oilspillcommission.gov/sites/default/files/documents/DEEPWATER_ReportothePresident_FINAL.pdf [01.12.2011]

Prillwitz, Fred/Krüger, Manfred: *Netzwiederaufbau nach Großstörungen.* In: Internet, 2007, unter URL: http://www.e-technik.uni-

rostock.de/ee/download/publications_EEV/eev_MarSymp2007_NWA.pdf [09.01.2012]

Saurugg, Herbert: *Der Cyberspace und die Auswirkungen auf die nationale Sicherheit*. Wien-Budapest: Corvinus Universität Budapest, Seminararbeit. 2011, (zit. 2011a)

Saurugg, Herbert: *Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit*. Wien-Budapest: Hochschule für Management Budapest (AVF), Seminararbeit, 2011, (zit. 2011b)

Toffler, Alvin: *Die dritte Welle.* München: Goldmann Wilhelm GmbH, 1997

Toffler, Alvin/Toffler Heidi: *Revolutionary Wealth*. New York: Knopf, 2006

VDE e.V.: *VDE Analyse Stromversorgungsstörungen in den USA/Kanada, London, Schweden/Dänemark und Italien/Anlässe und Abläufe, Ursachen und Konsequenzen.*In: Internet, 2003, unter URL: http://www.vde.com/de/fg/ETG/Pbl/Studien/Documents/MCMS/Blackoutbericht6.pdf [15.12.2011]

Vester, Frederic: *Die Kunst vernetzt zu denken.* München: dtv, 2011[8]

Witzer, Brigitte: *Risikointelligenz.* Berlin: Ullstein, 2011

Zeitung für kommunale Wirtschaft (Hrsg.): *Lehren aus den Blackouts/Hintergründe, Ursachen und Maßnahmen.* In: Internet, 2003, unter URL: http://www.zfk.de/zfk/knowhow/pdf_zum_nachlesen/hintergrund1203_03.pdf [30.12.2011]

Zukunftsforum öffentliche Sicherheit (Hrsg.): *Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland.* In: Internet, 2008, unter URL: http://www.zukunftsforum-oeffentliche-sicherheit.de/downloads/Gruenbuch_Zukunftsforum.pdf [04.12.2011]