Schriftenreihe Sicherheit

Aktueller Forschungsstand zur Verwundbarkeit kritischer Infrastrukturen am Beispiel der Stromversorgung

Kurzfassung

In Vorbereitung des zweiten Workshops im Oktober 2010 zum Thema „Konzept Kritische Infrastruktur: Vulnerabilitäten moderner Stromnetze und wie wir damit umgehen“ wurde im Auftrag des Forschungsforums die Expertise „State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall“ von PD Dr. Joern Birkmann et al., United Nations University, Institute for Environment and Human Security, Bonn, erstellt.

Stromversorgung ist nicht nur kritische Infrastruktur, sie ist **Basisinfrastruktur**, von der alle anderen Infrastrukturen abhängen. Daher ist die Frage der Vulnerabilität (Verwundbarkeit) dieser Infrastruktur von entscheidender Bedeutung.

VULNERABILITÄT - DREI ASPEKTE SIND BESTIMMEND

Nach einer Definition der United Nations International Strategy for Disaster Reduction versteht die Risikoforschung unter Vulnerabilität „physische, soziale, ökonomische und ökologische Faktoren und Prozesse, die die *Anfälligkeit* einer Gesellschaft gegenüber *Gefahren* (hazards) erhöhen“. Inzwischen wird das Konzept um die beiden Aspekte *Exposition* und *Bewältigung* erweitert, sodass sich folgende Betrachtung ergibt:

f (Vulnerabilität) = Exposition (Gefahr), Anfälligkeit, Bewältigungskapazität

Einige Faktoren haben sich in den letzten 20 Jahren grundlegend geändert: So hat die Strommarktliberalisierung seit 1998 zu einer Konzentration auf der ersten Versorgungsebene geführt: 80 Prozent der Elektrizität wird von den vier großen Verbundunternehmen EnBW, E.On, RWE und Vattenfall Europe erzeugt. Die Privatisierung ist mit einer unübersehbaren Anzahl von Akteuren – rund 1.100 Einzelunternehmen – verbunden. Das ehemals nationale und zentralisiert aufgebaute, staatliche Versorgungsnetz von 1,7 Millionen Kilometer Länge wird heute mit Anforderungen der freien Marktwirtschaft, des internationalen Strommarktes, der Proliferation von IT-Systemen sowie Schnittstellen zu anderen nationalen Netzen konfrontiert.

Die **Analyse der Vulnerabilität** und die daraus abgeleiteten **Handlungsmöglichkeiten** zur Förderung der Resilienz (Widerstandsfähigkeit) der kritischen Infrastruktur Stromversorgung sollen entlang der drei Bereiche Exposition, Anfälligkeit und Bewältigungskapazität skizziert werden.

EXPOSITION – GEFAHREN VON AUSSEN

Zu den Gefahren, die von außen das System stören können, zählen vor allem Naturgefahren und von Menschen verursachte Gefahren wie Terroranschläge und Cyberattacken. Eine Betrachtung ausgewählter Stromausfälle zeigt, dass weniger ein einzelnes und eindeutig zurechenbares Ereignis zu Störungen führt, sondern ein Zusammentreffen mehrerer Ereignisse, wie beispielsweise Kraftwerks- *und* Leitungsausfälle. **Naturgefahren** werden hinsichtlich ihrer geographischen Ausbreitung unterschieden: Hochwasser ist lokal begrenzt, eine Hitzewelle räumlich entgrenzt. In Bezug auf Handlungsmöglichkeiten ergeben sich unterschiedliche Strategien: Sensible Infrastruktur kann aus einem Hochwassergebiet verlegt werden; Erdkabel bieten ansonsten einen erhöhten Schutz, da Freileitungen gegenüber Extremwetter stärker exponiert sind. Terroranschläge

werden hauptsächlich im Zusammenhang mit Bedrohungen von AKWs thematisiert, da ein erfolgreicher Anschlag eine besonders starke Betroffenheit der Bevölkerung zur Folge hätte. Effektive Schutzmöglichkeiten von AKWs gibt es nicht. Auf die Stromversorgung selber hätte der Ausfall eines AKW keine ernsthaften Auswirkungen.

Eine besondere Gefahr für Stromversorgung scheint eher von **Cyberkriminalität** auszugehen. Der Ausbau der Stromnetze zu *smart grids* bedeutet eine höhere Exposition gegenüber Cyberattacken, die schon durch kleine, lokale Störungen große Auswirkungen induzieren können. Andererseits lassen sich durch intelligente Steuerungssysteme erneuerbare Energien besser nutzen sowie Energiequellen und Verteilnetze dezentralisieren. Beides trägt zu mehr Versorgungssicherheit bei. Empfohlen werden daher Strategien der **Komplexitätsreduktion** sowie der **Ausbau von Systemredundanzen**, um bei Störungen die Handlungsfähigkeit zu erhalten. Hier besteht großer Forschungsbedarf. Eine bessere Sensibilisierung der Unternehmen, bessere juristische Grundlagen und ein internationales Krisenmanagement wären weitere Schritte zu mehr Cybersecurity.

ANFÄLLIGKEIT – GEFAHREN UND PROBLEME VON „INNEN"

Mit der Anfälligkeit der Elektrizitätsversorgung sind systemimmanente Faktoren gemeint. Dazu zählen fünf Kernbereiche:

- Technologische Faktoren: Durch die mangelnde **Speichermöglichkeit** von Strom muss die Produktion nach wie vor *just in time* erfolgen. Derzeit wird versucht, über das Einbeziehen von Elektroautos, ein zukünftiges dezentrales Speichersystem zu entwickeln. Weiterhin wirkt sich in Unternehmen der Kostendruck auf Wartung, Pflege und Erneuerung aus. Ziel sollte die Entwicklung neuer Normen und die Verpflichtung der Betreiber auf bestimmte Sicherheitsleistungen sein.
- Institutionelle Faktoren: **Privatisierung** und **Liberalisierung** stellen ein weiteres Problem der Energieversorgung dar. Die heutige fast unübersehbare Zahl in- und ausländischer Akteure macht die Zurechenbarkeit von Verantwortung zunehmend problematisch. Kritisiert wird, dass die Integration des europäischen Stromnetzes vor allem unter Kostenaspekten und zu wenig unter Sicherheitsaspekten vorangetrieben wurde. Nach wie vor fehlt es an Handlungsempfehlungen und praktischen Umsetzungsmöglichkeiten für die Mitgliedstaaten. Das grundsätzliche Problem, dass eine systematische Planung zur Reduktion der Anfälligkeit den Zielen der freien Marktwirtschaft widersprechen kann, bleibt bestehen. Hier müssen neue Lösungsansätze entwickelt werden, an deren Gestaltung sowohl Betreiber, als auch Staat und Verbraucher teilhaben sollten.
- Die gesellschaftlichen Faktoren beziehen sich auf den nach wie vor steigenden Strombedarf (0,6% pro Jahr) und verändertes **Nutzerverhalten**, wie beispielsweise erhöhte Stromnachfrage bei Hitzewellen aufgrund von Klimaanlagen.
- Menschliche Faktoren, wie die **Kompetenz des Fachpersonals**, spielen ebenfalls eine Rolle. Ein Defizit an Koordination und bindenden Regeln zwischen den Betreibern für den Umgang mit Notfallsituationen und unzureichende Notfallpläne werden erwähnt.
- Systembezogene Faktoren: Die zunehmende **Komplexität** des Systems und die Ausweitung der IT-Infrastrukturdienstleistungen macht das Gesamtsystem immer schwerer berechenbar. So nimmt die Anzahl der Komponenten und die im Vorhinein oft nicht absehbare Kompatibilität zu. Die Vielzahl von **Abhängigkeiten** innerhalb des Systems kann schon bei geringen Störungen zu Domino- oder Kaskadeneffekten führen.

Ressourcenknappheit und **Klimaschutz** fordern einen massiven Ausbau der erneuerbaren Energien. Die wetterabhängige Stromproduktion der beiden Hauptenergielieferanten (Windkraft und Photovoltaik) muss mit grundlastfähigen Energieträgern (Wasserkraft, fossile Brennstoffe) flexibel kombiniert werden, um das Netz stabil zu halten. Dafür wird in immer größerem Maße IT-Steuerung benötigt.

Unter dem Gesichtspunkt der Verwundbarkeitsreduktion sollte der notwendige Umbau der Netze beforscht und Fragen der Investitionen und die Probleme mit Genehmigungsverfahren, z. B. für große Überlandleitungen, beantwortet werden.

BEWÄLTIGUNGSKAPAZITÄT – MÖGLICHKEITEN UND BEDINGUNGEN

Unter Bewältigungskapazität versteht man Möglichkeiten, die Umständen entgegenwirken, die zu einer Krise führen können. Zwei Kategorien sind zu unterscheiden: Zum einen technische, präventive Maßnahmen, und zum anderen reaktive Maßnahmen, die den Umgang mit Notfallsituationen betreffen.

Der **Faktor Umfeld** ist eine wichtige Einflussgröße: stabile politische und gesellschaftliche Verhältnisse wirken sich präventiv positiv aus. **Redundanzen**, die Reduktion des Wiederherstellungsaufwandes von Komponenten und Prozessen sowie die Bereitschaft (also der Grad der Vorbereitung auf Notfallsituationen, beispielsweise durch Übungen) sind Indikatoren für die reaktive Bewältigungskapazität. Ein sinnvoller Ansatz besteht hierbei in den regelmäßig durchgeführten LÜKEX-Übungen des Bundes und der Länder.

Der (n-1)-Sicherheitsstandard (eine technische Bestimmung für den Umfang redundanter Systeme, die zur Verfügung gestellt werden müssen) wird als nicht mehr ausreichend angesehen. Als Erweiterung wird in der Literatur der Austausch von **Echtzeit-Daten** empfohlen. Damit könnte das Fachpersonal der Kontrollstellen in Notsituationen über bessere Entscheidungsgrundlagen verfügen. Durch szenarienbasierte Übungen sollten Mitarbeiter entsprechende Kompetenzen schulen können.

- Bewältigung durch Risk Governance: Der **Risk Governance** Ansatz will die Verwundbarkeit der Elektrizitätsversorgung reduzieren, indem er die verschiedenen Akteure – Wirtschaft, Politik und Gesellschaft – in die Entscheidungsprozesse mit einbezieht. Eine Umsetzungsmöglichkeit bieten Public Private Partnerships (PPPs). In die Betrachtung der Risiken fließt neben der Verwundbarkeit als weitere Größe die Wahrscheinlichkeit mit ein, sodass idealerweise nach einem Abschätzungsprozess das akzeptierbare Restrisiko festgelegt und anschließend Managementmaßnahmen auf verschiedenen Ebenen (technische Ebene, Kontrollebene, institutionelle Ebene) ergriffen werden.
- Bewältigung durch Komplexitätsreduktion: Bisher sind die besonderen Bedingungen beim Umgang mit den komplexen Systemen der Kritischen Infrastrukturen wenig erforscht. Zwar versucht die Wissenschaft diese zu modellieren, doch die Ursache-Wirkungs-Komplexität bei Störungen und Ausfällen ist mittelfristig **beinahe nicht zu lösen**, da Verknüpfungen und Interdependenzen häufig nur qualitativ zu erfassen sind und sich viele logische und physische Verknüpfungen erst bei einem Ereignis wirklich offenbaren. Auch gibt es bisher nur Einzelberichte über größere Stromausfälle; eine systematische und vergleichende Auswertung aller Ereignisse fehlt. Konsens ist, dass Stromausfälle häufig nicht auf eine einzelne Ursache zurückzuführen sind, unklar aber ist, bei welchen Komponenten oder Prozessen die größeren Anfälligkeiten liegen.

FAZIT

Elektrizitätsversorgung und Stromausfall ist noch ein relativ junges Thema. Die erste politische Wahrnehmung der damit verbundenen Risiken geschah nach dem Anschlag auf das World Trade Center 1993. Seit 1997 gibt es in Deutschland eine interministerielle Arbeitsgruppe zu Kritischen Infrastrukturen. Publikationen des Bundesinnenministeriums (2005 und 2009) sowie das Grünbuch (2008) des Zukunftsforums Öffentliche Sicherheit haben das Thema immer mehr ins Zentrum der Aufmerksamkeit von Politik und Wissenschaft gerückt. In der Studie zeichnet sich ab, dass die Herausforderungen eher in der systemimmanenten Anfälligkeit der Versorgungssysteme und in den bisher mangelhaft entwickelten Bewältigungskapazitäten, als im Bereich der Exposition gegenüber Gefahren besteht. Dabei ist Anfälligkeit und Bewältigung nicht nur technisch zu verstehen. Die Studie mahnt mehrfach Defizite an, die durch den Übergang von der staatlichen zur marktwirtschaftlichen Versorgung entstanden sind. Auch die Tatsache, dass moderne Gesellschaften derzeit hochabhängig von nicht berechenbaren Infrastruktur-Systemen sind, offenbart Forschungsbedarf in präventive und reaktive Strategien. Welchen Stellenwert dabei die Bewältigungskapazität durch die Bevölkerung einnimmt oder einnehmen sollte, wurde hier nicht thematisiert und ist Gegenstand einer weiteren Studie des Forschungsforums.

Marie-Luise Beck
Projektkoordinatorin, Forschungsforum Öffentliche Sicherheit

Jörn Birkmann, Claudia Bach, Silvie Guhl, Maximilian Witting, Torsten Welle, Miron Schmude (2010): State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall
ISBN: 978-3-929619-63-8
Die Vollversion der Studie ist erhältlich unter www.schriftenreihe-sicherheit.de

Das 2009 an der Freien Universität Berlin gegründete Forschungsforum Öffentliche Sicherheit (www.sicherheit-forschung.de) führt Forschung unterschiedlicher Disziplinen zu sicherheitsrelevanten Themen zusammen und trägt dazu bei, zukünftig relevante Forschungsthemen zu identifizieren. Hauptsächlich geschieht dies durch Workshops und Expertisen zu verschiedenen Facetten der Sicherheitsforschung. Ziel ist es, wissenschaftliche Handlungsempfehlungen aus diesem heterogenen Feld zu generieren und für Politik, Industrie, und Organisationen der Sicherheit zugänglich zu machen. Die Idee zu diesem Projekt entstand auf Anregung des am Bundestag gegründeten Zukunftsforums Öffentliche Sicherheit e.V., dem Abgeordnete aller Parteien sowie Stakeholder aus Behörden, Wirtschaft und Wissenschaft angehören.

Forschungsforum Öffentliche Sicherheit
Freie Universität Berlin
GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

Impressum:
Forschungsforum
Öffentliche Sicherheit
Freie Universität Berlin
Fabeckstr. 15, 14195 Berlin
Tel: +49 (0)30 838 57367
Fax: +49 (0)30 838 57399
www.schriftenreihe-sicherheit.de
kontakt@schriftenreihe-sicherheit.de