Freie Universität Berlin

Forschungsforum Öffentliche Sicherheit

Dokumentation Workshop "Konzept kritische Infrastruktur: Vulnerabilität der Stromversorgung und wie wir damit umgehen"

26./27. Oktober 2010

Kurzversion
von Marie-Luise Beck

Die Versorgungssicherheit im Stromsektor in Deutschland ist noch hoch. Durch gesellschaftspolitische Veränderungen (Liberalisierung, Europäisierung), ökonomische Veränderungen (Privatisierung), aktuelle technische Veränderungen (Integration von Erneuerbaren Energien) und zukünftige Veränderungen (E-Moblity, Smart Grid-Technologien) entsteht Druck auf Sicherheitsstandards und Verlässlichkeit der Systeme. Gleichzeitig steigt die Abhängigkeit von verlässlicher Stromversorgung weiter an.

Der Workshop diente dazu, das Feld der Vulnerabilität von Stromversorgung sowie die derzeitigen technischen, gesellschaftlichen und politischen Bewältigungsstrategien zu beschreiben. Aus den gewonnenen Erkenntnissen wurden Handlungsempfehlungen abgeleitet.

Das Thema **Sensibilisierung der Bevölkerung** wurde vor allem in den Arbeitsgruppen mit den Schwerpunkten Bevölkerung und Kommunikation diskutiert. Die Experten kritisierten, dass es sich hierbei oft eher um ein Schlagwort, als um ein strategisches Konzept handelt. Gefragt ist eine **adressatengerechte Kommunikation**, die unterschiedliche Zielgruppen unterschiedlich anzusprechen vermag („recipient design"). In der Wirtschaft ist dies z. B. schon längst üblich. Es fehlt jedoch an empirischer Forschung, an „reliablen Daten" über die unterschiedlichen (Sub-)Gruppen in der Bevölkerung, ihre Informationsbedürfnisse, ihre Bewältigungspotenziale und ihre Mediennutzung, z. B. in einer Krise. Die Bereitstellung von Information ist aber noch keine Kommunikation. Sensibilisierung durch „monologische Belehrung" der Bevölkerung mit Flyern o.ä. erreichen zu wollen, wurde als unzeitgemäße und überwiegend wirkungslose „Aufklärung im Stile der 70er Jahre" bezeichnet. Vielmehr müssten „dialogische Kommunikationsformen" aufgebaut werden, in denen die Bevölkerung auf Augenhöhe mit den Verantwortungsträgern kommunizieren kann. Ziel muss eine „**kollektive Erörterung**" von Sicherheit und speziell von Schutzzielen sein. Als Modell stellte man sich **Kommunikations-Plattformen** vor, die, ähnlich wie bei den Themen Sterbehilfe oder Fortpflanzungstechnologie, den Diskurs partei- und interessenübergreifend - ohne Alarmismus und jenseits „medialer Aufgeregtheit" - initiieren können. Ziel der kollektiven Erörterung soll ein **gesellschaftlicher Konsens** in Bezug auf Bedrohungslagen, Sicherheitsanforderungen und den Umgang mit Unsicherheit sein.

Grenzen findet die Idee der Sensibilisierung der Bevölkerung da, wo sie zur **Externalisierung von Sicherheitsleistungen** auf den Bürger/die Bürgerin missbraucht wird. Die **Gewährleistungspflicht des Staates** in Bezug auf die Sicherheit kritischer Infrastrukturen, ist grundgesetzlich verankert. Zur Umsetzung dieser Staatspflichten wurden (a) die Verstaatlichung von Strukturen, (b) die Privatisierung von Strukturen unter der Voraussetzung definierter staatlicher Sicherheitsstandards ohne Einpreisung (Bsp. Singapur) und (c) die Privatisierung mit Einpreisung der Sicherheitsstandards diskutiert.

Neben der Sensibilisierung der Bevölkerung spielte die **Sensibilisierung von Verantwortungsträgern**, Experten und Wissenschaftlern ebenfalls eine Rolle. Krisenkommunikation zwischen und innerhalb von Behörden und Organisationen der Sicherheit, sog. Interorganisationsbeziehungen, muss etabliert, professionalisiert und geübt werden. Umgekehrt sollte eine **Aus- und Weiterbildung für Journalisten** zu Sicherheitsthemen und kritischen Infrastrukturen eingerichtet werden.

Die Arbeitsgruppe mit dem Schwerpunkt Technik nahm die technischen und gesellschaftlichen Bedingungen für **Versorgungssicherheit** zum Ausgangspunkt. **Erneuerbare Energien**, die zu Ressourcensicherheit und Klimaschutz beitragen, erhöhen gleichzeitig die *Un*sicherheit in Bezug auf die Stromversorgung aufgrund ihrer zeitlich und örtlich heterogenen Verfügbarkeit. Die Herausforderung besteht darin, die extremen Spannungsschwankungen im Netz durch IT-Steuerungstechnik auszugleichen. Der dadurch erforderliche Netzausbau ist in der Bevölkerung wie auch in der Wirtschaft aus je unterschiedlichen Gründen unpopulär. Diese Widersprüchlichkeiten bedürfen einer klareren Risikokommunikation. Die Experten forderten in einen „breiten Diskurs" Sicherheitserfordernisse zu definieren. Sie entwarfen einen **Anforderungskatalog an eine sichere Stromnetz-Architektur**. Zu den Hauptforderungen gehörte: (a) Robustheit und Zuverlässigkeit der Technik müssen Priorität gegenüber ökonomischen Zielen (z.B. Börse) haben, (b) Sicherheitsanforderungen müssen von Anfang an in die Technologieentwicklung integriert sein, (c) „so viel IT wie nötig und so wenig IT wie möglich, denn IT ist unsicher", (d) Implementierung neuer und Re-Implementierung alter Standards (z. B. n-1 Standard). Die Umsetzung müsse durch Regulierung sichergestellt werden. Die Alternativlosigkeit weiterer **Komplexitätssteigerungen technischer Systeme** wurde angezweifelt. Stattdessen wurden Konzepte der Selbstorganisation von Systemen, der Härtung kritischer Kernfunktionalitäten aber auch *low-tech* als Rückfalloption und Krisenbewältigungsinstrument diskutiert. Gleichzeitig betonte die Arbeitsgruppe, dass *high-tech* auch als Chance auf mehr Sicherheit zu betrachten sei. Geforscht werden müsse sowohl in Richtung *high tech*, als auch in Richtung *low tech*.

Auch die Idee der **Service Level Agreements** (SLAs) wurde angesprochen. Darunter versteht man die Akzeptanz unterschiedlicher Grade der Energiesicherheit zu unterschiedlichen Tarifen. Damit könnte sich eine gewisse Toleranz gegenüber Stromausfall (z. B. „eine Stunde pro Tag evtl. kein Strom, je nach Lastlage") ökonomisch rechnen. Noch ist unklar, wie und ob ein solches System „sowohl gesellschaftlich, technisch, organisational, wirtschaftlich und ökologisch lohnend einführbar" ist.

Ein weiterer Schwerpunkt, der vor allem die Arbeitsgruppe mit Schwerpunkt Politik beschäftigte, lag in der **Bewältigung eines langanhaltenden, großflächigen Stromausfalls.** Zwar ist die Eintrittswahrscheinlichkeit gering, die Risiken sind jedoch enorm. Die Behauptung, Ressourcen und Strukturen seien ausreichend vorhanden, wurde als Mythos bezeichnet. Als Hauptschwachpunkte wurden (a) ungenügende Notstromkapazitäten, (b) Probleme der Treibstoffzuführung und (c) der Zusammenbruch des IKT-Sektors nach 2-48 Stunden identifiziert. Der Legislative wurde die Überprüfung der Sicherheits- und Vorsorgegesetze sowie des Energiewirtschafts- und des Telekommunikationsgesetzes in Bezug auf Bewältigungskapazitäten und Sicherheitserfordernisse anempfohlen. Die Wissenschaft sollte die Vulnerabilitäts- und Folgenforschung ausbauen und stromausfallspezifische Schwachstellen bei Bewältigungskapazitäten in allen Sektoren überprüfen und identifizieren. Für den Fall eines Stromausfalls sollte eine „stromlose Krisenkommunikation" und andere Optionen aus dem low-tech-Bereich als Rückfalloption etabliert werden. Beispielsweise wäre die 100 Jahre alte Technik der Handy-zu-Handy-Kommunikation im Falle des Ausfalls der Mobilfunk-Basisstationen für nur 50 Cent pro Gerät integrierbar.