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

26./27. Oktober 2010

Dokumentation

Transkription der Präsentationen und der Abschlussdiskussion: Helga Jäckel
Zusammenfassung und Dokumentation: Marie-Luise Beck

Inhalt:

Forschungsforum Öffentliche Sicherheit,
Fabeckstraße 15, 14195 Berlin, Tel. +49 30 838 75247,
marieluise.beck@fu-berlin.de; www.sicherheit-forschung.de

Tagesordnung

Dienstag, 26. Oktober 2010

09:30 Uhr	Anmeldung und Begrüßungskaffee
10:00 Uhr	Einleitung **Prof. Dr. Jochen Schiller,** Projektleiter, Freie Universität Berlin

Vulnerabilitäten und Gefahren

10:15 Uhr	Einführung in das Thema, **Marie-L. Beck,** Freie Universität Berlin
10:25 Uhr **Studie des Forschungsforums**	„Kritische Infrastrukturen im Bereich Stromversorgung – State of the Art“ **PD. Dr.-Ing. Joern Birkmann/Claudia Bach**, United Nations University
10:45 Uhr **Expertenbeiträge**	„Auswirkungen eines Stromausfalls“ **Prof. Dr. Friedemann Wenzel,** Universität Karlsruhe „Vulnerabilität von Stromnetzen“ **Prof. Dr. Albert Moser**, RWTH Aachen u. Wiss. Beirat des Forschungsforums „Risikoanalyse des Bundes u. d. Länder“ **Peter Lauwe,** Bundesamt für Bevölkerungsschutz u. Katastrophenhilfe
11:45 Uhr	**Kaffeepause**
12:00 Uhr **Expertenbeiträge**	„Cyber War und kritische Infrastruktur“, **Dr. Sandro Gaycken**, TU Stuttgart „Netzintegration erneuerbarer Energien“, **Prof. Dr.-Ing. Harald Schwarz,** Brandenburgische TU Cottbus, u. Wiss. Beirat des Forschungsforums „Rettungskräfte und krit. Infrastruktur“ **Prof. Dipl.-Ing. Reinhard Ries**, Branddirektion Frankfurt u. Wiss. Beirat des Forschungsforums
13:00 Uhr	**Mittagessen**

Bewältigung – Bevölkerung und Politik

14:00 Uhr	Einführung in das Thema, **Dr. Lars Gerhold,** Freie Universität Berlin
14:10 Uhr **Studie des Forschungsforums**	„Kritische Infrastrukturen aus Sicht der Bevölkerung“ **Dr. Martin Voss/Daniel Lorenz,** KFS, Universität Kiel

14:30 Uhr **Expertenbeiträge**	„Risikokultur“, **Prof. Dr. Gerhard Banse**, Karlsruher Institut für Technologie „Sensibilisierung und Wahrnehmung“ **Dr. Rosemarie Stangl**, Sigmund Freud Privatuniversität Wien „Kommunikationsanforderungen für eine resiliente Infrastruktur“ **Prof. Dr. Ortwin Renn**, Universität Stuttgart „Netzsicherheit – eine Herausforderung für das Energierecht“ **Prof. Dr. Joh.-Christian Pielow,** Ruhr-Universität Bochum
15:30 Uhr	**Kaffeepause**
16:00 Uhr	**AG-Arbeit I:** Konstituierung und Beginn
18:00 Uhr	Poster Session & Pause
19:00 Uhr	Gemeinsames Abendessen

Mittwoch, 27. Oktober 2010

Erarbeitung der Themen

9:00 Uhr	**AG-Arbeit II** AG I: KRITIS und Bevölkerung –Selbstschutz und Sensibilisierung AG II: KRITIS und Kommunikation – interne u. externe Krisenkommunikation AG III: KRITIS und technische Möglichkeiten der Resilienz AG IV: KRITIS und institutionelle Anforderungen und Ressourcen *individuelle Kaffeepause*
12:30 Uhr	**Mittagessen**

Abschlussdiskussion

13:30 Uhr **14:00 Uhr**	Ergebnispräsentation im Plenum und **Abschlussdiskussion** mit Mitgliedern des Steuerungskreises Moderation: **Bettina Freitag, bundespolitische Korrespondentin**
15:30 Uhr	Verabschiedung

Ergebnisse der Arbeitsgruppen

(Bei den in Anführungszeichen gesetzten Textteilen handelt es sich um Zitate aus den Folien oder der Präsentation des Moderators.)

AG I: „Kritische Infrastrukturen (KRITIS) und Bevölkerung - Selbstschutz und Sensibilisierung", Moderation: Prof. Wolf R. Dombrowsky

Inhaltliche Schwerpunkte der AG-Arbeit

Referenzrahmen. Es gibt kein „One-for-all-Szenario". Die Dimension des Stromausfalls bestimmt über Maßnahmen der Bewältigung.

Bevölkerung als Akteur. „Der Begriff der Bevölkerung muss vor dem Hintergrund des Beziehungsgeflechts unterschiedlicher Akteure differenziert werden (z.B. Konsumenten, Produzenten, Politische Regulierung und ‚Profiteure'). Ebenso müssen Maßnahmen, die in Richtung Bevölkerung zielen, dieses Beziehungsgeflecht berücksichtigen."

Sensibilisierung der Bevölkerung als zentrales Thema. Die Sensibilisierung der Bevölkerung wurde als *das* zentrale Thema in der AG vertiefend diskutiert. Es wurde nach Gründen der Sensibilisierung, „derer, die sensibilisiert werden sollen und derer, die sich sensibilisieren lassen", gefragt. Ebenso wurde nach Konzepten der Sensibilisierung gefragt, die als je „unterschiedlich, und abhängig von dem Menschenbild und der intrinsischen Motivation" eingeschätzt wurden.

- **Begriffsbestimmungen: Sensibilisierung und Resilienz.** Beide Begriffe sind eher vermarktungsfähige Wortschöpfungen oder Modeworte, denn wissenschaftlich klare Begriffe. Der ursprüngliche Kontext dieser Begriffe wird im derzeitigen Diskurs der Sicherheitsforschung nicht thematisiert. Sensibilisierung und Resilienz ist in Abhängigkeit von Wissen / Bildung, von Reichtum / Einkommen zu sehen. Weiterhin hat Sensibilisierung eine „riskante Seite": Wie kann man Sensibilisierung optimieren, ohne die Bevölkerung ängstlich und unsicher zu machen („Risiken und Nebenwirkungen von Maßnahmen")? Wie kann man vorbereiten und warnen, ohne Panik zu schüren?
- **Sensibilisierung als kollektive Erörterung.** Sensibilisierung ist nicht mehr als monologische Belehrung oder (70er Jahre) „Aufklärung" möglich. Es müssen vielmehr „gemeinsame Verarbeitungsmodi" entwickelt werden, wie „mit Unsicherheit und Unbestimmtheit" umgegangen werden kann. Ansatzpunkt ist „eine kollektive Erörterung unterschiedlicher Szenarien". Daraus müssen kollektive (strukturelle Vulnerabilität betreffende) und individuelle (Wie weit will ich mich schützen?) Strategien abgeleitet werden. Ziel muss die Konturierung einer „kollektiven Sicherheit" sein.

- **Sensibilisierung setzt gesamtgesellschaftliche Bestimmung von Schutzzielen voraus.** Eine neue Qualität von Risiko bedeutet neue Anforderungen an die Risikobearbeitung. Die Definition von Schutzzielen „erfolgt vor dem Hintergrund der Tatsache, dass von Seiten der Produzenten weder Netzsicherheit noch Versorgungssicherheit bestimmbar sind. Auch auf Konsumentenseite (Haushalte und Nichthaushalte) sind die Gefährdungen und Reaktionsmöglichkeiten insbesondere bei längerfristigen Lagen nicht mehr eindeutig bestimmbar."

Technische Umsetzbarkeit von Schutzzielen. „Die allgemeinen Schutzziele sind im Gesetz [z. B. EnWG, Anm. M. B.] klar definiert, ihre derzeitige Umsetzbarkeit ist unklar und unzureichend. Die normativen Schutzziele sind stärker konturiert und klarer als das, was man technisch derzeit leisten kann. Diese Diskrepanz steigt zukünftig noch an (Datenverfügbarkeit und technische Kopplung von Systemen)."

Forschungsfragen / Forschungsfelder:

- Entwicklung partizipativer Forschungsmethoden zur Beförderung einer kollektiven Erörterung, um Sensibilisierung in der Bevölkerung zu erreichen und Schutzziele ableiten zu können.
- Entwicklung einer Methodologie der Befragung der Bevölkerung zu Katastrophenszenarien oder Lebenszusammenhängen, die sie noch nie erlebt hat, entwickeln.
  Weil es in der Bevölkerung keine Erfahrung mit großflächigen und komplexen Katastrophenlagen gibt, stellt sich die Frage, ob traditionelle Befragungs- und Evaluierungsmethoden überhaupt adäquat sind, „wenn es darum geht, herauszubekommen, was Bevölkerung über zukünftige Möglichkeiten denkt"?
- Differenzierung der Bevölkerung in unterschiedliche Subgruppen / Interessenlagen / Motivationen
- Entwicklung technischer Umsetzbarkeit von in Gesetzen definierten Schutzzielen.
- Systematische Evaluation/Auswertung bisheriger Forschungsprojekte.

Handlungsempfehlungen und Botschaften

- **Neue Arten der Risikowahrnehmung und Risikobearbeitung werden benötigt.** „Smart Grid" als zunehmend unbestimmbares, nicht mehr zurechenbares, integriertes und gekoppeltes System bedeutet eine neue Qualität von Risiko, auf die „neu" reagiert werden muss.

- **Die Sensibilisierung der Bevölkerung ist nur als kollektive Erörterung mit dem Ziel der Entwicklung einer „kollektiven Sicherheit" sinnvoll.**
  Darunter ist zu verstehen:
  - Diskussion individueller und struktureller Ursachen und Auswirkungen mithilfe partizipativer Methoden und anhand von Szenarien und
  - die Erarbeitung von Handlungsoptionen.
- **Ziel sollte eine ausgewogene Erörterung sein**, um „symbolische Aufgeregtheit" in Sicherheitsdiskursen zu vermeiden.

AG II: Kritische Infrastrukturen (KRITIS) und Kommunikation - interne und externe Krisenkommunikation (KK); Moderation Prof. Martin Löffelholz

Inhaltliche Schwerpunkte der AG-Arbeit

Referenzrahmen. Anforderungen bei Punktlagen und bei einem „totalen Stromausfall" wurden unterschieden. Die Frage, „Was kann Krisenkommunikation bei totalem Stromausfall leisten?", wurde gesondert erörtert.

Relevanz von Krisenkommunikation. Die AG konstatierte ein gestiegenes „Problembewusstsein und z.T. Aufwertung von Kommunikation als Funktion in Organisationen (z.B. Feuerwehr)." Problematisch sind „diffuse Vorstellungen von Krisenkommunikation". In Bezug auf Kompetenzen, Professionalität und der konkreten Umsetzung wurden Defizite identifiziert. Das Bewusstsein der Akteure dafür, dass KK entscheidend bei der Bewältigung einer Krise ist, muss gestärkt werden. Teilweise arbeiten Organisationen noch mit „veralteten Vorstellungen von Kommunikation."

Strategien und Instrumente der Krisenkommunikation: Es sollte „adressatengerecht" und „dialogisch" kommuniziert werden. „Einfachheit und Schnelligkeit der Kommunikation" sind wichtige Ziele. Die Umsetzung solcher Ziele ist das Problem. Hier gibt es noch keine Konzepte.

Zielgruppen differenziert ansprechen („recipient design"). „Bevölkerung als Adressat [ist] zu allgemein." Bevölkerung hat unterschiedliche Informationsbedürfnisse, die man kennen und ernst nehmen muss. „Ziel- bzw. Anspruchsgruppen [müssen] differenziert werden." Die besondere Ansprache von „Kindern und Jugendlichen (Kindergarten, Schulen, Erziehung, Anbindung an bestehende Konzepte- z.B. Notwehr und Krisenerziehung durch die Feuerwehr an Einrichtungen), älteren Mitbürgern, Kranken bzw. Krankenhauspersonal" sowie die Adressierung von „kulturellen Differenzen - z.B. Migranten, Touristen (Sprachen!); Stadt- und Landbevölkerung" müssen berücksichtigt werden.

KK bei „totalem Stromausfall". Dabei treten die technischen Aspekte in den Vordergrund: Welche Durchhaltefähigkeit, welche *back-up*-Systeme gibt es in den einzelnen Bereichen, z. B. den Öffentlich-

rechtlichen Rundfunksendern? Sollten Behörden sowie Polizei, Feuerwehr, THW etc. mit einem funktionierendem Kommunikationsnetz (z.B.. Satellitentelefon) ausgestattet werden? Sollte ein „flächendeckendes Sirenensystem“ zur Alarmierung der Bevölkerung wieder eingeführt werden? Welcher Art müsste die Warnung sein (z.B. Signal „weitere Infos am Sammelpunkt“)?

Interorganisationsbeziehungen: Wie können Behörden und Einsatzkräfte effizient *miteinander* und untereinander kommunizieren? Unterschiedliche Organisationstypen und –kulturen müssen berücksichtigt werden. Es gibt wenig Wissen über andere Organisationstypen, andere Kulturen. Die Ebenen Bund, Land, Kommune müssen berücksichtigt werden. Schon „ wenn der eine Landkreis mit dem anderen kommunizieren muss“, wird es schwierig. Aber auch die Aufsplitterung der privatwirtschaftlichen Unternehmen ist ein Problem („Das integrierte Energieversorgungsunternehmen ist tot.“).

Medien als Akteur akzeptieren. Medien sollte man als „wichtige Instanz in einer demokratischen Gesellschaft ernst nehmen“, aber nicht versuchen, sie als Partner zu missbrauchen. Die „Sicht von Medien als Gefahr [ist] weit verbreitet, aber wenig hilfreich“. Besser ist es, eine „Win-Win Situation“ herzustellen. Medien sollten bei der Vorbereitung auf Krisenkommunikation einbezogen werden. Hilfreich ist es, sie differenziert (z.B. Boulevard- vs. Qualitätsmedien) zu betrachten.

Forschungsfragen / Forschungsfelder:

- Aufbau empirischer Forschung zu Krisenkommunikation, insbesondere:
  - Beforschen der unterschiedlichen Informationsbedürfnisse, der unterschiedlichen Anspruchsgruppen in der Bevölkerung,
  - Beforschen der „Kommunikation innerhalb und zwischen den unterschiedlichen Organisationstypen“,
  - Erheben von validen Daten zur Mediennutzung unter Krisen- oder Katastrophenbedingungen.
- Erarbeitung eines Konzeptes adressatengerechter und dialogischer Kommunikation mit der Bevölkerung.
- Sicherstellung der „Anschlussfähigkeit von Krisenkommunikation an andere relevante Aspekte (z.B. Technik, Institutionen, etc.)“.
- Weiterentwicklung des Forschungsfeldes Risikokommunikation: „Wie kann das Bewusstsein der Bevölkerung über Notwendigkeit von Prävention geweckt werden?“

Handlungsempfehlungen und Botschaften

- **Bewusstsein stärken für die Relevanz einer professionellen Krisenkommunikation**, u. a. durch von der Politik initiierte Dialoge zwischen Staat, Rettungskräften und weiteren Verantwortlichen: „Nehmt Euch des Themas Krisenkommunikation mehr an!“
- **Die Krisenkommunikations-Kompetenz der Behörden und Einsatzkräfte** sollte verbessert und teilweise modernisiert werden, Kenntnisse über die Arbeitsweise der Medien sollten ausgebaut werden. Die „Bedeutung von Kommunikation und PR erkennen, Kommunikation als strategisches Werkzeug betrachten und Regeln exzellenter PR beachten (z.B. Medienbeziehungen aufbauen)“.
- Regelhafte **Aus- und Weiterbildungsangebote für Journalisten** zu kritischen Infrastrukturen und zu Sicherheitsthemen einzurichten wären angesichts der komplexen und abstrakten Thematik empfehlenswert.

AG III: „Kritische Infrastrukturen (KRITIS) und technische Möglichkeiten der Resilienz“, Moderation: Prof. Hermann J. Thomann, Dr. Leon Hempel

Inhaltliche Schwerpunkte der AG-Arbeit

Versorgungssicherheit. Die derzeitige Versorgungssicherheit wird als noch relativ hoch eingeschätzt, obgleich sie in den letzten Jahren leicht gesunken ist. Allerdings erzeugen gesellschaftspolitische Veränderungen (Liberalisierung, Europäisierung), ökonomische Veränderungen (Privatisierung) und technische Veränderungen (Integration von Erneuerbaren Energien, E-Moblity, Smart Grid-Technologien) zunehmenden Druck auf Sicherheitsstandards und Verlässlichkeit der Systeme. Gleichzeitig steigt die Abhängigkeit von verlässlicher Stromversorgung weiter an.

Redundanzen re-implementieren. Es geht nicht nur darum, wie Redundanzen geschaffen werden können, sondern auch darum, wie bestehende Standards erhalten bleiben können. Z. B. wie der „Leitsatz n-1 tatsächlich wieder in die Praxis“ umgesetzt werden kann. Denn „das Prinzip der n-1 Versorgung ist tatsächlich nicht mehr überall wirksam“. Technische Anforderungen an Versorgungssicherheit liegen „im Spannungsfeld von Zentralisierung und Dezentralisierung“. „Dezentralisierung bis zur Autarkie“ wäre keine Lösung, es sei denn man würde „Zuverlässigkeitseinbußen in Kauf nehmen“.

IT. Die zunehmend komplexen Systeme bzw. Anforderungen (z. B. verkürzte Reaktionszeiten bei Störungen) sind nur noch durch eine Ausweitung der IT-Steuerungstechnologie beherrschbar. Diese steigende Abhängigkeit von Automatisierungsprozessen führt zu neuen Risiken. Speziell IT-Experten der AG warnten vor „zu viel IT, weil IT unsicher ist“. Weiterhin vergrößert sich dadurch die Angriffsfläche für digitale Formen der Kriminalität wie Hacking etc.

Gesellschaftliche Anforderungen an Versorgungssicherheit. Es wird eine hundertprozentige Versorgungssicherheit von Bevölkerung, Fachwelt und Wirtschaft erwartet. Wegen der veränderten Rahmenbedingungen (s. o.) sollte in einem breiten Diskurs ein konkreter Anforderungskatalog erarbeitet werden, dessen Umsetzung durch Regulierung sichergestellt werden muss. Es stellte sich die Frage, ob Genehmigungsverfahren für den erforderlichen Netzausbau durch mehr „Transparenz und Beteiligung" beschleunigt werden könnten.

Service Level Agreements (SLA). Statt das Ziel der hundertprozentigen Sicherheit zu verfolgen, wäre auch eine ökonomische Perspektive denkbar: Unterschiedliche Grade der Verfügbarkeit werden unterschiedlich bepreist – sog. Service Level Agreements (SLAs). 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 diese „sowohl gesellschaftlich, technisch, organisational, wirtschaftlich und ökologisch lohnend einführbar" sind.

Erneuerbare Energien. Die Integration von Erneuerbaren Energien ist politisch gewollt, um den Klimawandel abzumildern und die Ressourcensicherheit zu erhöhen. Erneuerbare Energien erhöhen aber gleichzeitig die *Un*sicherheit in Bezug auf die Stromversorgung aufgrund ihrer zeitlich und örtlich heterogenen Verfügbarkeit. Auf diese Schwankungen muss mit dem Ausbau der Netze, der IT-Steuerungstechnologie und mit E-Energy-Konzepten reagiert werden.

Umgang mit steigernder Komplexität. Die Dynamik der Systeme nimmt weiter zu. Zum einen wegen ihrer physischen Größenzunahme der Netze (Europäisierung), zum anderen wegen der Integration von Erneuerbaren Energien. Aber auch die zukünftige Nutzung von Elektromobilität und die Einführung von Smart Grid werden zur dynamischen Weiterentwicklung beitragen, auch wenn Timing, Umfang und Tiefe noch unsicher sind. Daraus folgt: Der „künftige Netzbetrieb erfordert wesentlich dynamischere Modelle (Stichworte: Speicher durch E-Mobility)". Und: „Modellierung anhand mehrseitiger Szenarien der künftigen Stromversorgung [ist nötig] statt [ein Vorgehen nach] Trial & Error". Auch statistische Modelle reichen nicht mehr aus.

Kriterien für einen Anforderungskatalog an eine sichere Architektur. Die AG entwickelte erste Thesen zu Kriterien für einen Anforderungskatalog an eine sichere Architektur. (Die Idee eines Anforderungskataloges korrespondiert mit der Forderung nach einer „Kollektiven Erörterung" aus AG I.)

- Keine Vorgabe von konkreten Lösungen, sondern der prinzipiellen Eigenschaften, i. S. von Zielvorgaben.

- Kritische Kernfunktionalität muss besonders robust implementiert und garantiert werden. Dabei müssen
    - ökonomische Anforderungen (z. B. Börse) den Steuerungsanforderungen untergeordnet und
    - durch IT ausgelöste Probleme maximal begrenzt werden.
- Prinzipielle Differenzierung von Robustheitsanforderungen an verschiedene Ebenen und Schnittstellen. Denkbar wäre:
    - Verfügbarkeitsmaß, differenziert nach Abnehmern (Haushalte, Krankenhaus etc.),
    - Unterschiedliche Service Level Agreements (SLA).
- Der Widerstreit zwischen den Ebenen muss durch eine angepasste Architektur (Wettbewerb der Architekturen) kompensiert werden. Dazu gehört u. a.:
    - Sicherheitsanforderungen müssen in den Technikentwicklungsprozess integriert sein.
    - Keine statische Modellierung von IT-Sicherheit, stattdessen dynamischer *modus operandi* und jährliche Evaluation.
    - Robustheit in Bezug auf unterschiedliche Bedrohungen (Sturm, Hackerangriff, …).

Forschungsfragen / Forschungsfelder:

- Entwicklung von dynamischen Modellen, die die (neuen) komplexen Systeme simulieren und Wechselwirkungen modellieren können.
- Entwicklung von Architekturen, die durch Erneuerbare Energien induzierte Schwankungen ausgleichen können.
- Evaluation unterschiedlicher Architekturen / Teilarchitekturen.
- Erforschung von Akzeptanz / Akzeptabilität zukünftiger Techniken (SLAs, Smart Grid, E-Mobility, …).

Handlungsempfehlungen und Botschaften

- **Ein Anforderungskatalog an eine sichere Stromnetz-Architektur sollte in einem breiten Diskurs erarbeitet werden.** Es bedarf dabei der Konkretisierung rechtlicher und gesellschaftlicher Bedingungen (Qualitätssicherung, Rechtssicherheit, Datenschutz, Haftungsfragen…).
- Es sollte ein **Wettbewerb unterschiedlicher Architekturmodelle** initiiert werden.
- **Unsicherheit und Sicherheit im Zusammenhang mit Erneuerbaren Energien** muss klarer an die Bevölkerung kommuniziert werden.
- Die **(Re-)Implementierung von Sicherheitsstandards** in die Stromnetzarchitektur sollte politisch forciert werden.

AG IV: „Institutionelle Anforderungen und Ressourcen im Umgang mit Kritischen Infrastrukturen (KRITIS)“, Moderation Dr. Thomas Petermann

Inhaltliche Schwerpunkte der AG-Arbeit

Referenzrahmen. Die AG hat sich in ihren Überlegungen auf das Szenario großflächiger und langanhaltender Stromausfall bezogen, ein Szenario mit geringer Eintrittswahrscheinlichkeit , aber gravierenden Folgen (low probability – high risk), wie vor allem Kaskaden- und Dominoeffekten. Dadurch wären, relativ schnell sämtliche KRITIS betroffen.

Technische Achillesferse. Drei Systeme oder Strukturen wurden identifiziert, die der Bewältigung eines solchen Szenarios am meisten entgegenstehen:

1. Ungenügende Notstromkapazitäten,
2. Probleme der Treibstoffzuführung und
3. Zusammenbruch des Kommunikations-(IT-TK-)Sektors nach 2 bis 48 Stunden (je nach technischer Pufferkapazität).

Von diesen Schwachstellen sind Behörden, Unternehmen der Daseinsvorsorge sowie Hilfs- und Rettungskräfte gleichermaßen betroffen.

Das Krisenmanagementsystem ist geprägt durch eine unübersehbare Vielzahl und Heterogenität der privaten und staatlichen Akteure.

Knappheiten. Die ausreichende Verfügbarkeit von Ressourcen (und Strukturen) wurde als Mythos bezeichnet. Insbesondere die Notstromversorgung kritischer Infrastrukturkomponenten sei in Bezug auf ihre Verfügbarkeit, Kommunizierbarkeit, Robustheit und Durchhaltefähigkeit stark überschätzt.

Juristische Grundlagen. Die Sicherheits- und Vorsorgegesetze des Bundes bieten eine Reihe von Möglichkeiten, auf Strukturen und Güter zuzugreifen, jedoch wurden eine Zersplitterung und eine fehlende Harmonisierung diagnostiziert. Insbesondere dem Energiewirtschaftsgesetz und dem Telekommunikationsgesetz mangle es an Vorgaben notwendiger Bewältigungskapazitäten bzw. Sicherheitserfordernisse.

Bedingungen für Krisenkommunikation ohne Strom. Die Krisenkommunikationskonzepte bauen auf technischen Infrastrukturen auf, die im Falle eines Stromausfalls nicht mehr existieren. Welche Möglichkeiten der „stromlosen Kommunikation“ gibt es?

Forschungsempfehlungen / Forschungsfelder:

- Systematisches Screening derzeitiger Möglichkeiten von „stromloser Kommunikation".
- Nicht nur high-tech-, sondern auch **low-tech-**orientierte (pragmatische und finanzierbare) Lösungsmöglichkeiten für Krisenkommunikation schaffen.
  Beispiel: Das durch das Bundesministerium für Bildung und Forschung finanzierte Projekt „TankNotStrom" (http://www.bmbf.de/pub/Projektinformationen_TankNotStrom.pdf) bringt mit einfachem Mitteln Bedarf und Angebot zeitnah zusammen. Dieser Ansatz sollte auf andere Felder ausgedehnt werden.
- **Vulnerabilitätsforschung** und **Folgenforschung** sollten ausgebaut werden.
- Vulnerabilitäts- und Folgenforschung auch zu zukünftigen Entwicklungen wie *Smart Grid* bzw. **smarte Infrastrukturen** sollten ausgebaut werden

Handlungsempfehlungen und Botschaften

- **Krisenmanagement-Netzwerke etablieren und verstetigen**. Die verantwortlichen Akteure müssen sich in Kommunikationsnetzwerken zusammenfinden, die auf Dauer gestellt sind, um Verlässlichkeit, Vertrauen und Routinen zu etablieren. Gemeinsame Übungen sind ein Schlüssel zum Erfolg („Üben, üben, üben").
- **Katastrophenrelevantes Recht in Bezug auf Standardisierung, Harmonisierung und Sicherheitserfordernisse systematisch überprüfen.** Dies betrifft die Sicherheits- und Vorsorgesetze des Bundes und insbesondere das Energiewirtschafts- und das Telekommunikationsgesetz.
- **Low Tech.** „Konzepte für stromlose Krisenkommunikation" sollten als Rückfalloption etabliert werden.
- **Stromausfallspezifische Schwachstellen bei Bewältigungskapazitäten** sollten in allen Sektoren überprüft und identifiziert werden.

Abschlussdiskussion

Teilnehmer auf dem Podium:

- Prof. Dr. Wolf Dombrowsky, Soziologe, Steinbeis Hochschule Berlin, Leiter der AG I (Bevölkerung)
- Prof. Dr. Martin Löffelholz, Kommunikationswissenschaftler, Technische Universität Ilmenau, Leiter der AG II (Kommunikation)
- Prof. Dr.-Ing. Hermann Thomann, TÜV Rheinland Consulting GmbH, Vorsitzender des Zukunftsforums Öffentliche Sicherheit, , Leiter der AG III (Technik)
- Dr. Thomas Petermann, Büro für Technikfolgenabschätzung beim Deutschen Bundestag, Leiter AG IV (Politik)
- Gerold Reichenbach, Bundestagsabgeordneter und Mitgl. des Innenausschusses, Mitglied des Steuerungskreises des Forschungsforums Öffentliche Sicherheit
- Prof. Dr.-Ing. Jochen Schiller, Informatiker, Freie Universität Berlin, Projektleiter Forschungsforum Öffentliche Sicherheit
- Dr. Christine Thomas, Bundesministerium f. Bildung u. Forschung, i. V. Prof. Lukas, Mitglied des Steuerungskreises des Forschungsforums Öffentliche Sicherheit

Inhaltliche Schwerpunkte

- **Gesellschaftlicher Dialog.** Die Durchdringung aller Infrastrukturbereiche mit IT, die zunehmende Komplexität neuer technologischer und organisationeller Systeme machen eine Definition gesellschaftlicher Anforderungen an Sicherheit sowie politischer Setzungen (z.B. für Erneuerbare Energien, E-Mobility, …) nötig.
- **Daten und Datenverfügbarkeit für die Forschung.** Bevölkerung ist ein „wesentlicher Akteur“ im Feld Sicherheit. Es fehlt jedoch an zuverlässigen Daten. Als Problem erweist sich hier die mangelnde Datenverfügbarkeit für wissenschaftliche Zwecke. Diese Problematik war einigen Diskutanten neu. Sie müsste aber in den Datenschutzdiskurs Eingang finden. Das „Rechtsgut des Persönlichkeitsschutzes“ muss gegen andere Rechtsgüter abgewogen werden. Nicht hilfreich sind unterschiedliche Zuständigkeiten des Bundes und der Länder für den Datenschutz.

- **Forschungsstrategien im Sicherheitsbereich.**
    - Das Sicherheitsforschungsprogramm des BMBF (seit 2007) war nie reine Technologieförderung. Szenario-orientierte Projekte mit 10 und mehr Teilnehmern unterschiedlicher Disziplinen standen im Vordergrund. Dieser Ansatz soll im neuen Programm weitergeführt werden.
    - Sicherheitsforschung sollte in „beide Richtungen“ forschen: *Low-tech-Lösungen und High-tech-Lösungen*.

- *Low-tech-Lösungen*: Über Low-tech-Lösungen lassen sich – oft relativ kostengünstig - Rückfalloptionen für den Krisenfall implementieren. Ziel muss die Möglichkeit zur Selbstorganisation von (Teil-)Systemen sein. Beispiel: Handy zu Handy Funktechnik aus den 20er Jahren, könnte für 50 ct pro Handy integriert werden. Auch in Bezug auf Exportchancen, sollte man nicht nur in Richtung „Komplexität exportieren" denken. Viele Länder würden gerade einfache Systeme nachfragen. Auch low tech kann „smart" sein.
- *High-Tech-Lösungen:* Ist nicht zuletzt der „Verliebtheit von Forschern" in komplexe Systeme geschuldet. Gleichzeitig sind heutige Techniken zumeist manuell nicht mehr beherrschbar, sondern bedürfen vollautomatischer Prozesse. Neue Technologien sollten aber nicht nur in ihrem Risikopotenzial, sondern auch in ihrem Sicherheitspotenzial wahrgenommen werden. Beispiel: bei E-Mobility könnten Autobatterien auch als Puffer für Stromausfälle genutzt werden. Wenn Sicherheitsanforderungen von Anfang an in die Entwicklung neuer Technologien integriert werden, kann High-Tech unter Berücksichtigung einer robusten Kernfunktionalität als sichere Technik entwickelt werden.

Das anwendungsorientierte Sicherheitsforschungsprogramm des BMBF zielt in beide Richtungen; es geht um Systeminnovationen im High-Tech, aber auch im Low-tech-Bereich. Low-tech sollte als „Komplementärtechnologie" gesehen werden. Techniken mit Rückfalloptionen oder robuster Kernfunktionalität wären gerade auf dem Weltmarkt ein Unique Selling Point. Auch die Kombination von Sicherheitstechnologie mit politisch bereits gesetzten energiepolitischen oder klimapolitischen Zielen birgt Chancen.

- Die Problemstellungen ganz unterschiedlicher Krisenszenarien (Umwelt, Unternehmen, Terror, …) überlappen sich. Es sollte nach einem integrativen Ansatz gesucht werden.

- **Rahmenbedingungen für Forschung.** Forschung ist heute nur noch als national oder international organisierte und deshalb meistens programmatische Forschung möglich. Sie ist eingebettet in einen hohen Investitionsaufwand und in hohe Verwertungsrisiken. Die Forschungskonstitution des 21. Jahrhunderts ist eng verknüpft mit der Positionierung auf den Weltmärkten. Auch auf dem Gebiet der Forschung zeigt sich nationalstaatliche Entgrenzung. Sie korrespondiert gleichzeitig mit international verflochtenen (Forschungs-)Systemen, die eigentlich einen entsprechenden Verflechtungskontrollaufwand erforderten.
- **Bedingungen politischer und gesellschaftlicher Kommunikation aus Sicht der Politik.** Sensibilisierung für Sicherheitsthemen ist nur über Medienresonanz möglich. Eine Ausnahme bildet vielleicht die Kriminalitätsbedrohung, die der Bevölkerung am ehesten gegenwärtig ist. Die Politik benötigt einerseits konsistente Konzepte, *was* sie verändern will und andererseits ein mediales *back-up,* um Veränderungen im Bereich Sicherheit oder auch Katastrophenschutz durchzusetzen. Beispiel war nach der Elbe-Flut 2002 viel Geld und eine hohe Bereitschaft vorhanden, die Gesetze an die neuen Anforderungen anzupassen oder entsprechende Instrumente der Gefahrenabwehr zu implementieren. Aber es waren keine Konzepte in der Schublade. Heute sind - dank des Sicherheitsforschungsprogramms oder des Grünbuchs - die Themenfelder viel besser

beschrieben, sodass im Falle einer „Elbe 2002, die Zweite“ ganz andere Reaktionsmöglichkeiten zur Verfügung stünden.

- **Sensibilisierung der Experten.** Nicht nur die Sensibilisierung der Bevölkerung, sondern auch die Sensibilisierung der Experten (Wissenschaft, Behörden, Politik, …) müsse gestärkt werden. Nicht immer würden beispielsweise „so wenig IT wie möglich und so viel wie nötig“ implementiert, mit dem Ergebnis, dass die Produkte „immer wackliger“ würden.
- **Interdisziplinärer Ansatz in der Wissenschaft.** Um zukünftige Fragen der Sicherheitsforschung zu identifizieren bedarf es eines interdisziplinären, aber auch transdisziplinären (mit Politik, Endanwendern etc. verbundenen) Ansatzes. Die DFG beispielsweise fördert aber nach wie vor überwiegend disziplinär. Die Geistes- und Sozialwissenschaftler sind immer noch nur zu einem Bruchteil an den Sicherheitsforschungsprogrammen beteiligt. Die Gründe liegen nicht zuletzt auch in den Disziplinen selbst. Ein prominentes Beispiel sei die Krisenkommunikationsforschung. Es gibt wenig Ansatzpunkte oder Plattformen, die einen interdisziplinären Austausch ermöglichen. Das Forschungsforum Öffentliche Sicherheit wird deshalb als ein hilfreicher Ansatz gesehen. Mit dem Forschungsforum, das vor einem Jahr seine Arbeit aufgenommen hat, ist ein Prozess in Gang gekommen, den man gemeinsam weiter voran bringen sollte. Entscheidend für das Projekt selbst ist jetzt die Frage, wie man Kontinuität herstellen kann.
- **Interdisziplinärer Ansatz in der Politik fehlt.** Auch die Politik selbst muss sich stärker vernetzen. Manche Sicherheitsthemen werden im Wirtschaftsausschuss /-ministerium (z. B. Netzsicherheit), manche im Gesundheitsausschuss/-ministerium (z. B. Pandemie), manche im Innenausschuss/-ministerium (z. B. Krisenmanagement) etc. verhandelt.
- **Seriöse Sicherheitsdebatte mit dem Ziel eines gesellschaftlichen Konsenses.** Sicherheit, verstanden als gesellschaftliche Stabilität, sollte in ähnlicher Weise in der Öffentlichkeit verhandelt werden, wie es in anderen sensiblen Bereichen geschieht, z. B. in der Fortpflanzungstechnologie oder Sterbehilfe. Wir benötigen eine Kultur des Diskurses, jenseits der üblichen „Talkshow-Taktung“. Das Zukunftsforum Öffentliche Sicherheit, das 2007 seine Arbeit überfraktionell aufnahm, wird als ein Anfang gesehen.
  Benötigt wird eine Verbreiterung der Debatte, mit dem Ziel einen gesellschaftlichen Konsens zur Bedrohungslage zu erreichen. Ansonsten besteht die Gefahr, auf irrationale und teure Sicherheitslösungen zu setzen. Schon heute seien Ansätze zu „Schamanismus im Sicherheitsbereich“ zu beobachten.
  Das Thema „Stromausfall“ ist ein positives Beispiel für eine Thematik, die ohne allzu viel mediale Aufgeregtheit auf die Agenda gekommen ist. Dazu hat das Zukunftsforum entscheidend beigetragen. Ob sich das Thema auf der Agenda halten kann, ist noch offen.
- **Sicherheit im Stromnetz.** Um Redundanzen einstellen zu können, um die Auslastung der Netze nicht bis an die Kapazitätsgrenze zu fahren, muss in das Netz investiert werden. Die Zersplitterung von Zuständigkeiten und Akteuren seit Einführung der Liberalisierung und neuerdings durch das sog. Unbundling sind Risiken, denen Rechnung getragen werden muss. Die Rahmen-

setzung liegt letztlich in der Verantwortung der Politik.
Die politischen Handlungsoptionen lassen sich wie folgt skizzieren:

- Stromnetze, zumindest Teile davon, (wieder) verstaatlichen.
- Stromnetze in privater Hand lassen, aber Sicherheitsleistungen gesetzlich festlegen. (So geschehen in Singapur, wo nur mit Firmen Verträge zur Zulieferung geschlossen werden, die sich verpflichten, selbst im Kriegsfall, 6 Monate die Zulieferung aufrecht zu erhalten. Die Kosten dafür dürfen nicht eingepreist werden).
- Modelle, nach denen die Unternehmen die (zusätzlichen) Sicherheitsleistungen, z. B. über erhöhte Gebühren einpreisen.

- **Sicherheitsgewährleistungspflicht.** Sie zählt zu den grundgesetzlichen Aufgaben des Staates. Dazu gehört auch die Sicherheit überlebenswichtiger Infrastrukturleistungen. Der Gesetzgeber ist hier in der Verantwortung. Sensibilisierung der Bevölkerung darf nicht so verstanden werden, dass eine Externalisierung von Sicherheitsleistungen auf die BürgerInnen erfolgt.
- **Handlungsempfehlungen gefragt.** Nachdem das Feld der Vulnerabilität von Stromnetzen nun abgesteckt ist, gilt es, die gewonnenen Erkenntnisse aus der gemeinsamen Perspektive von Politik, Wissenschaft und Anwendern in handlungsfähige Maßnahmen zu überführen.