Einführung in das Schwerpunktthema

Resilienz und Vulnerabilität von Infrastrukturen

Von Astrid Aretz und Bernd Hirschl

Das moderne Leben und Wirtschaften beruht maßgeblich auf einer funktionierenden Infrastruktur, die in den letzten Jahren und auch in naher Zukunft einem gravierenden Wandel unterworfen ist, beziehungsweise sein wird. Von ursprünglich „analoger Hardware“ verändern sie sich durch den Einsatz von Informations- und Kommunikationstechnik (IKT) zu digital unterstützten Systemen.

Digitalisierung wird somit zu einem zentralen Treiber der Veränderung der Infrastrukturen, die gleichzeitig auch eine stärkere Kopplung der Infrastrukturen ermöglicht. Diese Kopplung ist vor allem aus Sicht des Energiesystems vorteilhaft, da auf diese Weise Nutzenergie- und Energiespeicherpotenziale infrastrukturübergreifend gehoben werden können.

Komplex und verwundbar

Durch die zunehmende Digitalisierung aller Infrastrukturen werden diese jedoch auch deutlich komplexer und damit verwundbarer gegenüber potenziellen Ausfällen. Dies potenziert das Gefährdungspotenzial in erheblichem Maße und unterstreicht die Notwendigkeit, einen lang anhaltenden, großflächigen Blackout zwingend zu verhindern. Die hohe Verwundbarkeit wird unter anderem durch die große Bandbreite und Vielzahl von Hackerangriffen auf kritische Infrastrukturen, darunter viele Unternehmen und Anlagen im Energiebereich, deutlich.

Die Verwundbarkeit beziehungsweise Vulnerabilität beschreibt dabei die Anfälligkeit des Systems und seiner Dienstleistung in Bezug auf konkrete interne und externe Störungen beziehungsweise auf strukturell bedingte Schwachstellen im System (Gleich et al. 2010). Ausfälle sind besonders bei den kritischen Infrastrukturen (KRITIS) mit wichtiger Bedeutung für das staatliche Gemeinwesen eine Gefahr. Deren Ausfall oder Beeinträchtigung kann nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen mit sich bringen (BMI 2009). Zu den kritischen Infrastrukturen zählen beispielsweise die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr sowie Gesundheit (BBK 2017).

Katastrophale Folgen

Die katastrophalen Folgen eines längeren großflächigen Stromausfalls wurden unter anderem ausführlich vom Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) analysiert und die Ergebnisse in der Studie „Was bei einem Blackout geschieht – Folgen eines langandauernden und großräumigen Stromausfalls“ dargestellt (Petermann et al. 2011).

Durch die Abhängigkeit aller Infrastrukturen und insbesondere der kritischen Infrastrukturen von einer funktionierenden Stromversorgung würden sich die Folgen eines langandauernden und großflächigen Stromausfalls sofort in allen Infrastrukturen niederschlagen. Mittels umfassender Folgenanalysen führen die Autoren vor Augen, dass bereits nach wenigen Tagen im betroffenen Gebiet die bedarfsgerechte Versorgung der Bevölkerung mit (lebens)notwendigen Gütern und Dienstleistungen nicht mehr sicherzustellen ist.

Dienstleistungen unter herausfordernden Umständen

Wie jedoch ein Infrastruktursystem auf Stress von außen oder Turbulenzen reagiert und ob es zu Ausfällen von Teilen oder der gesamten Infrastruktur kommt, hängt von deren Resilienz ab. Die Resilienz beschreibt die Fähigkeit eines Systems, die Dienstleistung auch unter diesen herausfordernden Umständen aufrechterhalten zu können (Gleich et al. 2010). Die Resilienz eines Systems ist jedoch nicht messbar, insbesondere da ein resilientes System auch mit unvorhersehbaren Ereignissen, den „unknown unknowns“ oder „Schwarzen Schwänen“, umgehen können muss.

*Ökologisches*Wirtschaften 4.2017 (32) | DOI 10.14512/OEW320414

Man kann aber aus prinzipiellen Überlegungen Eigenschaften und Komponenten eines resilienten Systems identifizieren, die sich zur Ableitung von Gestaltungsprinzipien nutzen lassen: Widerstandsfähigkeit, Anpassungsfähigkeit, Innovationsfähigkeit und Improvisationsfähigkeit (Stührmann et al. 2012).

In diesem Schwerpunkt sollen Verwundbarkeiten, die durch die Umgestaltung unserer Infrastrukturen entstehen, aufgezeigt und Ansätze diskutiert werden, wie damit umgegangen werden kann.

Zunächst geht ***Ulrike Lechner*** allgemein auf die Kategorien der Verwundbarkeiten kritischer Infrastrukturen ein. Die Autorin verdeutlicht auch, wie allgegenwärtig Angriffe auf die Informationstechnik (IT) in kritischen Infrastrukturen bereits heute schon sind, auch wenn die Bundesregierung von der das IT-Sicherheitsgesetz und andere Verordnungen mit dem Ziel eingeführt wurden, die kritischen Infrastrukturen zu den sichersten weltweit zu machen.

Ulrich Petschow und ***Jens Libbe*** verdeutlichen, welche Chancen sich durch die Digitalisierung für eine engere Verbindung der Infrastrukturen bieten. Mit dieser Sektorkopplung können Synergien (etwa bei der Vernetzung verschiedener Träger erneuerbarer Energien) und zum Teil auch größere Effizienzen erzielt werden. Gleichzeitig können mit der Kopplung auch zusätzliche Verwundbarkeiten auftreten, weil sich Ausfälle direkt auf andere Infrastrukturen übertragen. Die Autoren geben einen Überblick, welche Chancen sich durch die Sektorkopplung ergeben könnten, welche potenziellen Verwundbarkeiten durch die digital gestützte Kopplung auftreten und zu beachten sind und mit welchen Strategien diesen begegnet werden kann.

Danach beleuchten ***Astrid Aretz, Bernd Hirschl, Mark Bost, Mariela Tapia*** und ***Stefan Gößling-Reisemann*** die spezifischen Eigenschaften des Energiesektors. Dieser Sektor steht mit der Energiewende vor einem fundamentalen Umbruch und gerade deshalb bieten sich hier Chancen, die Systemarchitektur so zu gestalten, dass Resilienzstrategien frühzeitig implementiert werden.

Marc Schelewsky und ***Weert Canzler*** beschreiben die Trends im Verkehrssektor, beispielsweise die nutzerfreundliche Verknüpfung der verschiedenen Verkehrsmittel. Durch die Vernetzung erhöht sich jedoch die Zahl der externen Zugriffs- und damit auch Angriffspunkte zwangsläufig. Das gilt gleichermaßen für den Betrieb, als auch den Datenschutz und die Sicherheit der Nutzerdaten.

Während sich die vorangegangenen Artikel alle mit den Vulnerabilitäten aus technischer Sicht beschäftigen, beleuchten ***Daniel F. Lorenz*** und ***Marie Bartels*** die spezifische Anfälligkeit von Bürgerinnen und Bürgern in Form sozialer Vulnerabilität. Deren Bewältigungsfähigkeiten können als soziale Resilienz verstanden werden, mit der Schadenspotenziale minimiert werden können. Weiterhin gehen die Autor/innen auf Ansatzpunkte für eine aktive Risikokommunikation zur Verknüpfung von technischer und sozialer Perspektive ein.

„Durch die zunehmende Digitalisierung aller Infrastrukturen werden diese komplexer und verwundbarer gegenüber Ausfällen."

Literatur

BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) (2017): Sektoren und Branchen Kritischer Infrastrukturen (KRITIS). www.kritis.bund.de

BMI (Bundesministerium des Innern) (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Berlin.

Gleich, A. von/Gößling-Reisemann, S./Stührmann, S./Woizeschke, P./Lutz-Kunisch, B. (2010): Resilienz als Leitkonzept – Vulnerabilität als analytische Kategorie. In: Fichter, K./Gleich, A von/Pfriem, R./Siebenhüner, B. (Hrsg.): Theoretische Grundlagen für erfolgreiche Klimaanpassungsstrategien. Bremen, Projektkonsortium nordwest2050. 13–49.

Petermann, T./Bradke, H./Lüllmann, A./Poetzsch, M./Riehm, U. (2011): Was bei einem Blackout geschieht – Folgen eines langandauernden und großräumigen Stromausfalls. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). Berlin.

Stührmann, S./Gleich, A. von/Brand, U./Gößling-Reisemann, S. (2012): Mit dem Leitkonzept Resilienz auf dem Weg zu resilienteren Energieinfrastrukturen. In: Decker, M./Grundwald, A./Knapp, M. (Hrsg.): Der Systemblick auf Innovationen – Technikfolgenabschätzung in der Technikgestaltung. Berlin, edition sigma. 181–192.

AUTOR/INNEN + KONTAKT

Dr. Astrid Aretz ist Wissenschaftlerin am Institut für ökologische Wirtschaftsforschung (IÖW) im Forschungsfeld Nachhaltige Energiewirtschaft und Klimaschutz.

Institut für ökologische Wirtschaftsforschung (IÖW) GmbH, Potsdamer Str. 105, 10785 Berlin. Tel.: +49 30 884594-0, E-Mail: astrid.aretz@ioew.de, Website: www.ioew.de

Prof. Dr. Bernd Hirschl ist Leiter des Forschungsfelds „Nachhaltige Energiewirtschaft und Klimaschutz" am Institut für ökologische Wirtschaftsforschung (IÖW) und Stiftungsprofessor an der Brandenburgischen Technischen Universität (b tu) Cottbus-Senftenberg.

Institut für ökologische Wirtschaftsforschung (IÖW) GmbH, Potsdamer Str. 105, 10785 Berlin. Tel.: +49 30 884594-0, E-Mail: bernd.hirschl@ioew.de, Website: www.ioew.de

Brandenburgische Technische Universität Cottbus-Senftenberg, Großenhainer Straße 57, 01968 Senftenberg. Tel.: +49 3573 85-534. E-Mail: bernd.hirschl@b-tu.de, Website: www.b-tu.de/fg-energieversorgungsstrukturen