Digitaler Stillstand

Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven

ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN

Projektbericht Nr. 2017-01 | ISSN: 1819-1320 | ISSN-Online: 1818-6556

Digitaler Stillstand

Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven

Endbericht

Institut für Technikfolgen-Abschätzung
der Österreichischen Akademie der Wissenschaften

Projektleitung: Walter Peissl

Autoren: Stefan Strauß
Jaro Krieger-Lamina

Studie im Auftrag des Präsidiums der Österreichischen Akademie der Wissenschaften

Wien, März 2017 (überarb. Fassung v. Juni 2016)

IMPRESSUM

Medieninhaber:
Österreichische Akademie der Wissenschaften
Juristische Person öffentlichen Rechts (BGBl 569/1921 idF BGBl I 130/2003)
Dr. Ignaz Seipel-Platz 2, A-1010 Wien

Herausgeber:
Institut für Technikfolgen-Abschätzung (ITA)
Strohgasse 45/5, A-1030 Wien
www.oeaw.ac.at/ita

Die ITA-Projektberichte erscheinen unregelmäßig und dienen der Veröffentlichung der Forschungsergebnisse des Instituts für Technikfolgen-Abschätzung.
Die Berichte erscheinen in geringer Auflage im Druck und werden über das Internetportal „epub.oeaw" der Öffentlichkeit zur Verfügung gestellt:
epub.oeaw.ac.at/ita/ita-projektberichte

ITA-Projektbericht Nr.: 2017-01
ISSN: 1819-1320
ISSN-online: 1818-6556
epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.pdf

Inhalt

Abbildungs- und Tabellenverzeichnis

Zusammenfassung/Summary

Kritische Infrastrukturen als Hauptschlagadern der Gesellschaft

Die Funktionsfähigkeit gesellschaftlicher und wirtschaftlicher Prozesse ist heute hochgradig von verschiedenen Technologien und deren Zusammenspiel abhängig. Sie bilden dabei „kritische Infrastrukturen“, ein Begriff, der seit einigen Jahren an Bedeutung gewinnt. Kritische Infrastrukturen (KI) können als „Hauptschlagader“ von Wirtschaft und Gesellschaft verstanden werden. Dementsprechend schwerwiegend sind Ausfälle von Systemen, die zentral für die Funktionsfähigkeit der Daseinsvorsorge und Grundversorgung mit lebensnotwendigen Gütern sind. Unsichere Infrastrukturen gefährden das Funktionieren der Gesellschaft und damit die gesamte Bevölkerung. Zur Bewältigung dieser Herausforderungen gibt es eine wachsende Anzahl politischer Programme und Strategien zu diesem Thema auf europäischer und nationaler Ebene. Die Bedrohungslage ist insgesamt komplex und entsteht durch zwei miteinander verwobene Aspekte: Externe Risikofaktoren und systemimmanente Fehlerquellen. Eine Differenzierung und explizite Berücksichtigung beider Aspekte ist wesentlich, um die komplexe Sachlage besser verstehen und mit sinnvollen Maßnahmen bewältigen zu können. Insbesondere die Problematik von Systemabhängigkeiten ist bislang unterrepräsentiert. Eine stärkere Fokussierung darauf ist daher dringend notwendig. Die steigende Abhängigkeit wirkt sich letztlich negativ auf die Selbstorganisationsfähigkeit aller gesellschaftlichen Akteure (staatliche und private Institutionen, Unternehmen, Zivilgesellschaft, Bevölkerung etc.) aus, die jedoch essentiell ist, um Krisen aller Art bewältigen zu können. Eine Reduktion der Abhängigkeit geht daher einher mit einer Stärkung des Problembewusstseins und der Resilienz der Gesellschaft.

Stromnetz als Basis-Infrastruktur

Informations- und Kommunikationstechnologien (IKT) als Querschnittstechnologien

Der vorliegende Bericht befasst sich mit wesentlichen Herausforderungen für den Schutz kritischer Infrastrukturen und der Problematik der zunehmenden wechselseitigen technologischen Abhängigkeit in diesem Feld. Die hohe Komplexität der Thematik legt eine Fokussierung auf spezielle Bereiche nahe. Daher wurden vor allem zwei zentrale Querschnittstechnologien in den Blick genommen: Das Stromnetz als kritische Basis-Infrastruktur, von der praktisch alle anderen Bereiche abhängen, sowie Informations- und Kommunikationstechnologien (IKT) und deren Bedeutung für die Vulnerabilität (Verwundbarkeit) kritischer Infrastrukturen. Der Fokus der Untersuchung liegt auf Österreich, wobei die globale Perspektive schon aufgrund der untersuchten Risiken immer wieder deutlich wird.

Elektromagnetische Impulse (EMP) und Sonnenstürme als mögliche Risiken

Untersucht wurden zunächst Risiken, die äußerst selten sind, aber massiven und schwer abschätzbaren Schaden für Stromnetz und IKT anrichten können: Elektromagnetische Impulse (EMP) und Sonnenstürme (als spezielle Form von EMP). Künstlich erzeugte EMPs bedürfen zur Erzeugung in der Regel militärischer Ressourcen wie Nuklearwaffen[1]. Zwar mag das

[1] Man spricht dann von sogenannten NEMPs, also durch Nuklearexplosion erzeugte EMPs.

Bedrohungspotenzial für Österreich aufgrund seiner geopolitischen Lage und Neutralität hier als eher gering gelten. Allerdings können EMPs mit neuartigen HPM[2]-Waffen mit geringerem Aufwand erzeugt und für gezieltere Angriffe eingesetzt werden. Solarstürme und Weltraumwetterphänomene sind ebenfalls selten, deren Risiken können aber nicht politisch reduziert werden. Österreich ist durch seine geographische Lage deutlich weniger gefährdet als etwa die USA oder Skandinavien. Trotz ihrer Unwahrscheinlichkeit ist eine Berücksichtigung verschiedener EMP-Risiken sinnvoll, da bislang wenig über die potenziellen Auswirkungen auf heutige Infrastruktursysteme bekannt ist. Evident sind etwa Stromausfälle (mitunter beschädigte Transformatoren), Störungen der Satellitenkommunikation und des Flugverkehrs. Hier besteht dementsprechend international weiterer Forschungsbedarf für Frühwarnsysteme und die Erforschung ihrer Auswirkungen. Es ist nicht eindeutig, inwieweit bestehende Richtlinien zur elektromagnetischen Verträglichkeit (EMV) vor EMPs schützen können. Ebenso unklar ist, inwieweit hier faktisch wirksame Schutzmaßnahmen getätigt wurden, um kritische Infrastrukturen abzusichern. Hinzu kommt, dass durch eine generelle Zunahme an vernetzten Geräten mit mehr elektromagnetischen Störquellen zu rechnen ist.[3]

Forschungsbedarf für Frühwarnsysteme

EMPs und Solarstürme sind zudem exemplarische Risiken, um die Problematik technologischer Abhängigkeiten zu verdeutlichen, die mit weiterer Vernetzung zunehmen und die Gefahr von Kaskadeneffekten und größeren Folgeschäden deutlich verschärfen. Neben EMPs bestehen zunehmende Risiken durch gezielte Angriffe auf IT-Systeme (Cyber-Angriffe) von kritischen Infrastrukturen. Möglich werden solche Angriffe vor allem durch mangelnde Sicherheitskonzepte. Kritische Infrastrukturen, die übers Internet direkt erreichbar sind, stellen grundsätzlich ein massives Sicherheitsrisiko dar. Angreifer können Schwachstellen etwa gezielt ausnützen, um Schadsoftware (Trojaner, Viren etc.) einzuspeisen. Derartige Fälle sind belegt und reichen vom Virenfund in Atomkraftwerken bis zum großflächigeren Stromausfall durch gezielte Angriffe. Neben Angriffen gibt es hier auch erhebliche Gefahren durch mitunter unbekannte Systemfehler. Es besteht daher insgesamt Bedarf nach verbesserten Schutzkonzepten von kritischen Infrastrukturen. Das bedeutet mehr Bewusstsein von Sicherheitsstandards und deren Umsetzung. Das erfordert mehr IT-Expertise für den Schutz kritischer Infrastrukturen sowie verstärkten inter- und transdisziplinären Austausch, um mehr Wissen über die Unterschiede und Gemeinsamkeiten von Energie- und IKT-Netzen zu erlangen. Mittel- und längerfristig gibt es weiters Bedarf nach Innovationen, die die Systemsicherheit in Design und Architektur insgesamt erhöhen (Security-by-design). Hierbei ist auch ein stärkerer Dialog zwischen Wissenschaft, Wirtschaft und Politik wichtig.

Risiko von Cyber-Angriffen

Bedarf nach mehr IT-Expertise für den Schutz kritischer Infrastrukturen sowie nach mehr inter- und transdisziplinärem Austausch

---

[2] High Power Microwave – Hochleistungsmikrowellenstrahlung.

[3] In Deutschland wurde daher kürzlich ein neues Gesetz zur elektromagnetischen Verträglichkeit von Betriebsmitteln beschlossen: heise.de/newsticker/meldung/Bundesregierung-will-das-Netz-der-elektrischen-Dinge-neu-regeln-3198356.html.

Für das Erkennen und Beheben von Abhängigkeiten ist Wissen über Schnittstellen und das Zusammenspiel unterschiedlicher Infrastrukturkomponenten erforderlich. Die Faustregel lautet: Schnittstellen erhöhen die Komplexität des Systems und machen es somit potenziell anfälliger. Nicht in Sicherheitskonzepten berücksichtigte Schnittstellen können dementsprechend unbekannte Risiken in sich bergen. Im Rahmen der Untersuchung wurden auch verdeckte Abhängigkeiten identifiziert, über die noch relativ wenig Problembewusstsein herrscht: Die Abhängigkeit von GPS (Global Positioning System) und anderen Satellitensystemen. Diese werden neben der Navigation mittlerweile in vielen Bereichen eingesetzt, so auch zur Zeitsynchronisation. Diese Systeme können auch in Transformatoren und Umspannwerken integriert sein und bei Ausfall zu erheblichen Störungen führen und sollten daher stärker bei der Analyse kritischer Infrastrukturen berücksichtigt werden. Im Hinblick auf die absehbar weiter zunehmende Vernetzung und Automatisierung (z. B. Industrie 4.0, Smart Grids, Smart Home, autonome Fahrzeuge, Internet der Dinge etc.) ist davon auszugehen, dass integrierte Systeme generell weiter an Bedeutung gewinnen werden. Dies wird Systemabhängigkeiten grundsätzlich weiter verschärfen und damit auch die Verwundbarkeit dieser Systeme. Dafür sind mehr Problembewusstsein und Vulnerabilitätsanalysen notwendig, um kritische Komponenten zu erkennen und diese in Folge, abhängig vom konkreten Risiko, besser zu schützen.

GPS als Risikoquelle

Systemabhängigkeiten steigen durch Vernetzung und Automatisierung

Mehr Problembewusstsein und Vulnerabilitätsanalysen notwendig

Das Österreichische Programm zum Schutz kritischer Infrastrukturen (APCIP[4]) beinhaltet strategische Maßnahmen, um die Resilienz Österreichs zu erhöhen. Hier wurde bereits einiges geleistet und Österreich zählt hier zu den Vorreitern in der EU. Eine Vielzahl an Strategien und Akteuren widmet sich der Thematik, was auf ein breites Problembewusstsein hindeutet. Diese Pluralität verdeutlicht einerseits die Komplexität der Problematik, bringt aber andererseits auch Unklarheiten hinsichtlich Kompetenzen und Zuständigkeiten mit sich. Der von Österreich gewählte funktionsorientiert-kooperative Ansatz zum Schutz kritischer Infrastrukturen zwischen Staat und Wirtschaft ist sinnvoll, um Sicherheit und Resilienz kritischer Infrastrukturen in Österreich zu stärken, und orientiert sich an der EU-EKI-Richtlinie[5]. Das APCIP fokussiert auf kritische Infrastrukturen, womit eine Abgrenzung zum SKKM besteht: APCIP versteht sich als Ansatz, der staatliches Krisen- und Katastrophenschutzmanagement (SKKM) nicht ersetzt, sondern erweitert; etwa durch die Entwicklung umfassender Konzepte zum Risiko-, Krisen- und Sicherheitsmanagement. Um eine etwaige „Verdopplungsgefahr" zwischen APCIP und SKKM zu vermeiden, sollte auf Synergien zwischen beiden Ansätzen, sowie die Präzisierung der jeweiligen Besonderheiten und Anforderungen (etwa der jeweils unterschiedlichen Beurteilung bzw. Bedeutung von Katastrophen und Krisen) geachtet werden. Eine Analyse (und gegebenenfalls Adaptierung) des Krisen-

Funktionsorientiert-kooperativer Ansatz in Österreich

Private-Public-Partnership

[4] Austrian Programme for Critical Infrastructure Protection.

[5] EU-Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

und Katastrophenschutzmanagements in Hinblick auf Überschneidungen, Synergien und Ressourcen mit APCIP und vice versa ist daher zweckmäßig und wird empfohlen.

Standards der Krisenkommunikation in technischer wie auch organisatorischer Hinsicht zentral

Der funktionsorientierte Ansatz Österreichs setzt stark auf die Eigenverantwortung der KI-Betreiber. Daher sind Standards im Sicherheitsmanagement bzw. betrieblichen Krisenmanagement besonders relevant. Hierbei sollte evaluiert werden, inwieweit Anpassungsbedarf besteht. Krisenkommunikation ist jeweils zentral. Kritische Faktoren sind mangelnde Interoperabilität und Kompatibilität etwa aufgrund unterschiedlicher Standards in technischer wie auch organisatorischer Hinsicht (z. B. mögliche Unterschiede zu Behördenfunksystemen anderer Staaten). Eine Überprüfung und ggf. Verbesserung von Standards zur Krisenkommunikation auch in Hinblick auf IKT-Abhängigkeiten wird daher empfohlen.

Krisenrobuste Funktechnologie

Bei einem Ausfall informationstechnischer Systeme ist mit Störungen oder Nicht-Verfügbarkeit digitaler Kommunikationsnetze zu rechnen. Um die Kommunikation weiterhin zu ermöglichen, sind Alternativen erforderlich. Als krisenrobustes Kommunikationsmittel gilt insbesondere die Funktechnologie. Es sollte daher die Verfügbarkeit und Nutzbarkeit von Funktechnologie unter allen relevanten Akteuren auch im Krisenfall sichergestellt werden, sodass die Krisenkommunikation zwischen den Akteuren möglichst friktionsfrei funktioniert.

Empfehlungen

Die Stärkung der Selbstorganisationsfähigkeit aller gesellschaftlichen Akteure und der Bevölkerung (Bewusstseinsbildung) ist insgesamt zentral für den Schutz kritischer Infrastrukturen. Das erfordert ein Zusammenspiel aller relevanten Akteure und Umsetzung von Maßnahmen. Die sich aus dieser Analyse ergebenden wichtigsten Empfehlungen sind:

- Kritische Zusammenschau vorhandener Aktivitäten und Planungsszenarien, d. h. Evaluierung der Unterschiede, Gemeinsamkeiten und Synergien von staatlichem Krisen- und Katastrophenschutzmanagement und dem Programm zum Schutz kritischer Infrastrukturen;
- Erfassung, Gewährleistung und Dokumentation der Verfügbarkeit von Notfallressourcen, insb. von
  - Notstromaggregaten bei KI-Betreibern und in kritischen Einrichtungen (z. B. im Gesundheits- und Sozialwesen);
  - Krisenkommunikationssystemen zur raschen Koordination aller relevanten Akteure und
  - Kommunikationskanälen zur Information der Bevölkerung unter Einbeziehung der Zivilgesellschaft
- Stärkung des Problembewusstseins für IT-Sicherheit und technologische Abhängigkeiten; Schnittstellen gelten dabei als neuralgische Punkte mit potenziellen Risiken in kritischen Infrastrukturen;
  - Bewusstseinsbildung und Hilfestellung bei der Umsetzung entsprechender Standards von KI-Betreibern
  - Erstellung von (Offline-)Notfallplänen

- Durchführung von Vulnerabilitätsanalysen kritischer Infrastrukturen (insbesonders im Stromnetz und kritischer Komponenten wie Transformatoren) zur
  - Identifizierung von Schwachstellen, vor allem von Abhängigkeiten zu anderen Systemen (IKT) und ggfs.
  - Erhöhung des Schutzniveaus durch
  - Reduktion von kritischen Abhängigkeiten durch bewusstes Schaffen von Redundanzen
- Evaluierung und eventuell Anpassung von Standards und Richtlinien
  - im Krisen- und Katastrophenschutzmanagement und
  - zur elektromagnetischen Verträglichkeit (EMV);
- Stärkung von Wissenschaft und Forschung in den Bereichen:
  - Sicherheit kritischer Infrastrukturen, Security-by-design, steigender Vernetzung und Systemabhängigkeit zur Entwicklung von wirkungsvollen Schutzmaßnahmen,
  - Interdisziplinäres Systemwissen und entsprechender (Aus-)Bildung zur gesellschaftlichen Bewältigung der Problematik,
  - Frühwarnung für geomagnetische Sonnenaktivität und elektromagnetische Felder, um Reaktionszeiten zu verringern und
  - Wirkungsforschung dieser Phänomene, um Auswirkungen besser einschätzen und Schutzmechanismen entwickeln zu können.

1 Einleitung

Die Gesellschaft hat sich innerhalb der letzten zwanzig Jahre mit fortschreitender Technisierung und rasanter Verbreitung neuer Technologien (insbesondere von Informations- und Kommunikationstechnologien – IKT) erheblich verändert. Die Funktionsfähigkeit gesellschaftlicher und wirtschaftlicher Prozesse ist heute hochgradig von verschiedenen Technologien und deren Zusammenspiel abhängig. Dadurch entstehen neue Herausforderungen für das Funktionieren dieser Prozesse. Im Hinblick auf das hohe Schadenspotenzial bei Ausfällen lassen sich einige dieser Bereiche unter dem Begriff „kritische Infrastruktur" (KI) zusammenfassen, der seit einigen Jahren an Bedeutung gewinnt. Es sind Ansätze zu entwickeln, um mit diesen Herausforderungen besser umgehen zu können. Die Herausforderungen sind dabei grundsätzlich globaler Natur, erfordern jedoch auch Problembewusstsein und Konzepte zur Bewältigung auf nationaler und regionaler Ebene. Dieser Bericht, der im Rahmen des Projekts „Digitaler Stillstand"[6] entstand, befasst sich mit einigen dieser Herausforderungen. Dieser Begriff ist eine metaphorische Reminiszenz auf Paul Virilio's (1992) Buch „Rasender Stillstand", in dem er u. a. die technologisch und medial beförderte Beschleunigung der Gesellschaft vorausschauend kritisch hinterfragt. Allerdings ist der Konnex dieses Berichts damit nur teilweise verwandt. Das Hauptaugenmerk liegt hier vielmehr darauf, die Verletzlichkeit der Gesellschaft als eine wesentliche Nebenwirkung des rasanten technischen Fortschritts (und insbesondere durch IKT und Digitalisierung) zu beleuchten. IKT und Digitalisierung sind in dieser Hinsicht kritisch, da IKT einerseits für die Funktionsfähigkeit der Gesellschaft wesentlich sind, andererseits, weil die Digitalisierung die bereits inhärente Komplexität kritischer Infrastrukturen noch weiter erhöht. Zwar kann digitale IKT in Summe in vielen Bereichen erheblich zur besseren Steuerung von kritischen Infrastruktursystemen beitragen (z. B. durch automatisierte Steuerungssysteme, Fernwartung etc.). Allerdings nimmt mit der erhöhten Komplexität auch die Anfälligkeit für Ausfallrisiken insgesamt zu, was sich etwa in zusätzlichen Abhängigkeiten, gesteigerter Fehleranfälligkeit, bis hin zu gezielten Angriffen niederschlagen kann.

Kritische Infrastruktur (KI) als zentraler Begriff

Aufgrund der enormen Vielschichtigkeit und Komplexität des Themas wurde eine Fokussierung auf spezielle Bereiche und Teilaspekte vorgenommen. Die Breite des Begriffs kritische Infrastruktur ist zwar zweckmäßig, um auf die Vielschichtigkeit der Problematik hinzuweisen, stellt aber zugleich eine Hürde für eine Konkretisierung dar, die nötig ist, um mehr Einblick in die Verwundbarkeit (Vulnerabilität) von Systemen zu erlangen, deren Ausfall für Gesellschaft und Wirtschaft kritisch werden kann. Die große Spannweite spiegelt sich im öffentlichen und fachlichen Diskurs wider, wo Black-

Fokussierung auf Vulnerabilität von IKT und Stromnetzen und deren Wechselwirkungen

[6] Mit dem Titel „Digitaler Stillstand" soll die Abhängigkeit der Gesellschaft von digitalen Systemen verdeutlicht werden, die in dieser Studie ausführlich behandelt wird. Nicht zuletzt wird dabei auf die steigende Verwobenheit von IKT und kritischer Infrastruktur – etwa in Form des Stromnetzes – verwiesen.

out-Szenarien durch Ausfall von Stromnetzen ebenso diskutiert werden wie Bedrohungen durch einen Cyber-War. Ein breiter Diskurs ist zwar grundsätzlich wichtig, ist alleine aber nicht ausreichend, um das tatsächliche Gefahrenpotenzial genauer zu beleuchten und sinnvolle Schutzmaßnahmen zu setzen. Im Gegenteil kann die Vermischung unterschiedlicher Bedrohungen und diverser Ausfallrisiken dabei mitunter die Identifikation von Vulnerabilitätsfaktoren und infolgedessen das Ableiten von Maßnahmen zur Verbesserung der Sicherheit erschweren. Es erscheint daher erforderlich, den Themenkomplex von einer systemischen Perspektive aus zu beleuchten, um nicht einzelne KI-Bereiche, sondern vielmehr technische Systeme, die in allen Bereichen relevant sind zu berücksichtigen. Informations- und Kommunikationstechnologie spielt hier eine Doppelrolle: Einerseits stellen IKT-Systeme selbst eine kritische Infrastruktur dar, andererseits handelt es sich dabei auch um eine Querschnittstechnologie, die in vielen anderen kritischen Infrastrukturen für deren Funktionieren erforderlich ist. Eine vergleichbare Rolle spielt das Stromnetz. Ebenfalls für sich selbst als kritische Infrastruktur zu betrachten, durchdringt es, vielleicht noch mehr als IKT, alle Infrastrukturen und Bereiche einer modernen Gesellschaft. Obendrein zeigt sich, dass sich diese beiden Technologien nicht nur wie ein roter Faden durch alle kritischen Infrastrukturen ziehen, sondern auch in enger Wechselwirkung zueinander stehen. Mit der fortschreitenden Digitalisierung und Vernetzung bildet sich gerade in diesen beiden Bereichen eine Hyperkonnektivität ab, die erhebliche Auswirkungen auf Systemarchitekturen mit sich bringt. Zum einen können vernetzte Systeme zur Erhöhung von Redundanzen beitragen. Zum anderen nimmt aber mit wachsender Vernetzung die Komplexität von kritischen Infrastrukturen zu, was zu neuen Systemabhängigkeiten und steigender Vulnerabilität führen kann.

Um die Thematik fassbarer zu machen, wurden im Rahmen dieser Studie daher vor allem zwei zentrale Aspekte in den Blick genommen:

Zentrale Aspekte

- Das Stromnetz als prominentes Beispiel für eine zentrale kritische Infrastruktur, von der praktisch alle anderen Bereiche abhängen.
- Die Bedeutung von IKT in kritischen Infrastrukturen bzw. inwieweit durch IKT die Vulnerabilität kritischer Infrastrukturen erhöht wird.

Der Anspruch ist hierbei nicht, eine detaillierte Risiko-Analyse dieser Bereiche vorzunehmen, sondern vielmehr, aus einer systemischen Meta-Perspektive die Problematik und ihre Implikationen zu analysieren.

Forschungsleitende Fragestellungen, die im Lauf der Studie untersucht wurden:

Forschungsfragen

- Welche Einflussfaktoren sind relevant für die Vulnerabilität kritischer Infrastrukturen und welches Bedrohungspotenzial entsteht durch neuartige bzw. bislang wenig beachtete Risiken?
- Welche zentralen Auswirkungen haben Systemabhängigkeiten und welche Abhängigkeiten sind besonders kritisch?
- Welche Implikationen hat ein Systemausfall bzw. Systeminstabilität?

- Welche relevanten Programme und Akteure gibt es in Österreich für den Schutz kritischer Infrastrukturen?
- Inwieweit gibt es Bedarf nach verbesserten Schutzmaßnahmen bzw. Stärkung des Krisenmanagements?

Methoden

Zur Untersuchung dieser Fragen wurde relevante Literatur (neben Fachartikeln auch Strategiedokumente und Forschungsberichte) recherchiert und ausgewertet. Ein systemtheoretischer Ansatz dient als Forschungsheuristik, um den Themenkomplex kritische Infrastruktur und die Problematik wechselseitiger Abhängigkeiten aus systemischer Perspektive zu beleuchten. Um zusätzliche Einsichten und Perspektiven zu gewinnen, wurden ExpertInneninterviews geführt und qualitativ ausgewertet. Zudem wurde ein Workshop mit ExpertInnen aus unterschiedlichen Bereichen (insbesondere SicherheitsexpertInnen aus Ministerien, öffentlicher Verwaltung und Unternehmen) durchgeführt.[7] Das Workshop-Format folgte einem „Constructive TA“[8]-Ansatz, bei dem verschiedene Stakeholder und ExpertInnen über Probleme und mögliche Lösungsansätze eines Themenbereichs diskutieren. Im Workshop wurde die Vulnerabilität kritischer Infrastrukturen in drei thematischen Blöcken behandelt. Mittels Szenario-Technik wurde mit den TeilnehmerInnen über Vulnerabilitätskriterien, Herausforderungen des Krisenmanagements bei Blackout und großflächigerem Internet-Ausfall sowie Systemabhängigkeiten diskutiert. Die aus Interviews und Workshop gewonnenen Erkenntnisse wurden bei der Ausarbeitung des Forschungsberichts berücksichtigt. Der Fokus der Untersuchung lag auf Österreich, wobei freilich die globale Perspektive schon aufgrund der Besonderheit der untersuchten Risiken dabei weitgehend berücksichtigt wurde.

Struktur des Berichts

Der Bericht geht in Kapitel 2 zunächst auf die Vulnerabilität kritischer Infrastrukturen ein und skizziert wesentliche Merkmale und Indikatoren für das bessere Verständnis kritischer Infrastrukturen. Kapitel 3 befasst sich mit Ausfallrisiken kritischer Infrastrukturen und Einflussfaktoren. Nach einer kurzen Übersicht werden Gefahren durch elektromagnetische Impulse und Solarstürme als besondere Form von Risiko näher erläutert. In Kapitel 4 werden die Relevanz der Systemperspektive und die Problematik von Systemabhängigkeiten erörtert. Ein Fokus liegt dabei auf dem Stromnetz als Basisinfrastruktur, in Folge werden informationstechnische Systemabhängigkeiten kritischer Infrastrukturen näher beleuchtet sowie diesbezügliche Angriffspotenziale. Kapitel 5 bietet eine Übersicht zu den wichtigsten Strategien und Akteuren im Bereich Schutz kritischer Infrastrukturen und deren Zusammenspiel. Im Anschluss werden Aspekte und Maßnahmen zur Stärkung der Resilienz erläutert. Das finale Kapitel 6 fasst die wichtigsten Herausforderungen zusammen und präsentiert Empfehlungen, die im Zuge dieser Untersuchung erarbeitet wurden.

---

[7] Dabei fiel auf, dass der Frauen-Anteil in dieser ExpertInnen-Community äußerst gering zu sein scheint. Auf die Wichtigkeit einer stärkeren Integration von Frauen in diesen Bereich sei deshalb an dieser Stelle hingewiesen.

[8] Konstruktive Technikfolgenabschätzung.

2 Vulnerabilität kritischer Infrastrukturen

Ein Großteil der gesellschaftlichen Grundversorgung mit Gütern und Dienstleistungen des täglichen Lebens basiert auf dem Zusammenspiel sogenannter kritischer Infrastrukturen (KI). Das Österreichische Bundeskanzleramt[9] definiert kritische Infrastrukturen als

Definition kritischer Infrastrukturen

> „jene Infrastrukturen (Systeme, Anlagen, Prozesse, Netzwerke 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 und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen haben würde“ (BKA 2015).

Diese Definition deckt sich weitgehend mit jener der Europäischen Union in der Richtlinie zu europäischen kritischen Infrastrukturen (EKI)[10], die darauf abzielt, das Problembewusstsein zum Schutz kritischer Infrastrukturen zu verbessern und das Schutzniveau zu erhöhen. Die Mitgliedstaaten sind aufgefordert, kritische Komponenten zu identifizieren und gegebenenfalls verbesserte Schutzmaßnahmen zu entwickeln.[11] Auf EU-Ebene ist hier bereits einiges passiert, u. a. widmet sich die Organisation ENISA[12] (European Union Agency for Network and Information Security) in ihren Arbeitsschwerpunkten verstärkt auch dem Schutz kritischer Infrastrukturen. Gleiches gilt für das Joint Research Center (JRC) der Kommission. Das JRC koordiniert etwa das European Reference Network for Critical Infrastructure Protection (ERNCIP)[13], zur Unterstützung und Wissensaustausch zwischen den EU-Mitgliedsstaaten. Auch auf nationaler Ebene wurde vieles geleistet. Alle EU-Mitgliedstaaten haben die Richtlinie rechtlich insofern erfüllt, als sie Prozesse zur Identifizierung kritischer Infrastrukturen gestartet haben (EUC 2012). Einige europäische Länder (z. B. Deutschland, Finnland, Großbritannien, Niederlande, Österreich, Schweden, Spanien, Schweiz) haben dazu auch nationale Programme entwickelt. Dennoch ist der Umsetzungsstand der EKI-Richtlinie noch im Fluss. Konkretere ope-

---

9 Ende 2014 wurde in Kooperation zwischen Bundeskanzleramt und Bundesministerium für Inneres das Österreichische Programm zum Schutz Kritischer Infrastrukturen beschlossen.

10 EU-Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008“ über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

11 Allerdings basieren die Bestrebungen auf EU-Ebene bislang primär darauf, kritische Infrastrukturen im Allgemeinen vor terroristischen Bedrohungen zu schützen. Die Problematik zunehmender Systemabhängigkeiten durch steigenden Vernetzungsgrad spielte dabei bislang keine gesonderte Rolle. Wenngleich die Gefahren von Terrorismus zweifelsohne relevant sind, erscheint es zur besseren Beherrschung der Gesamtproblematik zentral, Systemabhängigkeiten verstärkt zu berücksichtigen. Nicht zuletzt, da gezielte Angriffe dementsprechend Kaskadeneffekte auslösen könnten.

12 www.enisa.europa.eu.

13 ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection.

rative Maßnahmen gehen aus den nationalen Strategien nur ansatzweise hervor und befinden sich noch im Entwicklungsstadium. Ein wesentlicher Grund ist hierbei die enorme Komplexität der Materie sowie der nötige Zeit- und Ressourcen-Aufwand zur Identifizierung kritischer Infrastrukturkomponenten. Das stellte auch die Kommission bei der Evaluierung der Richtlinien-Umsetzung fest (EUC 2012). Der Ansatz der Richtlinie wird daher fortgeführt und weiter ausgearbeitet, wobei verstärkt auch auf Interdependenzen zwischen kritischen Infrastrukturen, Industrie und öffentlichem Sektor fokussiert werden soll (EUC 2013).

Zur Ermittlung kritischer Infrastrukturen gibt es verschiedene Ansätze. Das deutsche Bundesministerium des Innern versteht (zunächst ähnlich wie Österreich) unter kritischer Infrastruktur: „*Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.*“ (BMI/BSI 2009). In Deutschland werden kritische Infrastrukturen jedoch nach Sektoren unterschieden. Der österreichische Ansatz verzichtet dagegen bewusst auf eine sektorale Trennung und ist eher funktionsorientiert (vgl. BKA 2015). Das heißt, neben Bereichen der staatlichen Daseinsvorsorge werden Unternehmen und Einrichtungen von strategischer Bedeutung zu KI-relevanten Funktionsträgern gezählt (siehe Abschnitt 5). Allerdings erscheint eine Übersicht der relevanten Sektoren dennoch zweckmäßig, um die Breite des Begriffs KI besser fassen zu können. Wie die folgende Grafik veranschaulicht, umfassen KI eine Reihe unterschiedlicher Gesellschaftsbereiche, die von Lebensmittel- und Energieversorgung, Transport und Verkehr, Telekommunikation, Medien, Finanz- und Versicherungswesen bis zu Sozial- und Gesundheitswesen reichen:

Relevante Sektoren

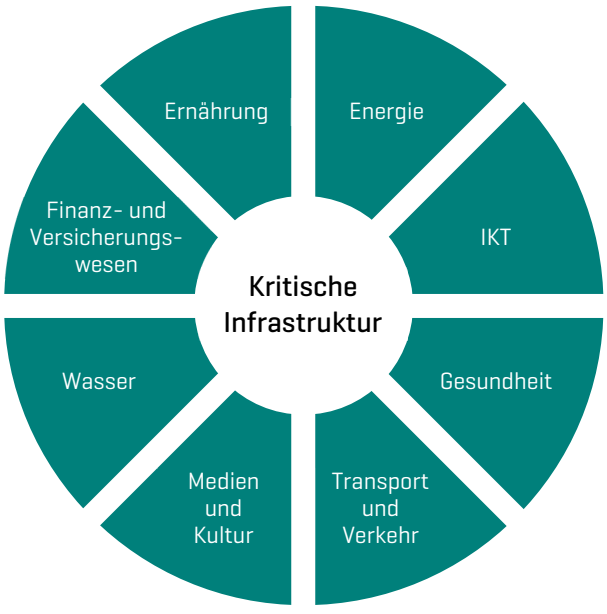

Abbildung 1: Sektoren kritischer Infrastrukturen
Quelle: adaptiert von BSI (2014, S. 5)

KI als zentrales Element staatlicher Daseinsvorsorge und essentiell für die wirtschaftliche Funktionsfähigkeit

All diese Bereiche sind für das Funktionieren der Gesellschaft von enormer Wichtigkeit. Ausfälle einer oder mehrerer Infrastrukturkomponenten in diesen Bereichen können dementsprechend schwerwiegende Folgen mit sich bringen. Die Verwundbarkeit von Infrastrukturen ergibt sich insbesondere auch aus der Fülle an Funktionen und Diensten, die sie erfüllen. Als Funktionsträger gesellschaftlicher Abläufe sind sie zentrales Element staatlicher Daseinsvorsorge und essentiell für die wirtschaftliche Funktionsfähigkeit. Störungen oder Ausfälle kritischer Infrastrukturen können dementsprechend erheblichen gesellschaftlichen und wirtschaftlichen Schaden anrichten. Diese können etwa durch Naturkatastrophen, technische Unfälle, menschliches Versagen, Gefahren im Cyberspace, Kriminalität und Terrorismus entstehen. Der Schutz kritischer Infrastrukturen ist daher wesentlich, um das Funktionieren von Gesellschaft und Wirtschaft zu gewährleisten.

Zwei Bereiche nehmen hier einen besonderen Stellenwert ein, da sie als Querschnittsmaterie in praktisch allen Sektoren für deren Funktionsfähigkeit maßgeblich sind: Die Energie-Versorgung und Informations- und Kommunikationstechnologien (IKT). Die hohe gesellschaftliche Abhängigkeit von Energie und Information zieht sich durch sämtliche Lebensbereiche hindurch und betrifft Industrie-Anlagen und Unternehmen ebenso wie private Haushalte. Die Folgen von Ausfällen etwa bei der Stromversorgung können dementsprechend sehr weitreichend sein und auch alle möglichen Alltagsgüter wie Heizung, Lichtversorgung, Kühlschränke, Fahrzeuge, Internet und Mobiltelefonie etc. betreffen. Durch den hohen Verbreitungs- und Vernetzungsgrad von IKT kann wiederum auch die Energieversorgung massiv gestört werden. (Abschnitt 4 befasst sich genauer mit der Problematik der Systemabhängigkeiten).

2.1 Merkmale von Vulnerabilität

Vulnerabilität bezeichnet *„… the conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards*." (UN/ISDR 2004, 16). Dieser Definition zufolge betrifft Vulnerabilität all jene Zustände, die die Anfälligkeit der Allgemeinheit für Gefahren erhöhen, was von einer Reihe von Faktoren, (physikalischen, sozialen, ökonomischen und Umweltfaktoren) abhängt. Eine zentrale Frage zur Erfassung von Vulnerabilität ist daher, wie anfällig kritische Infrastrukturen für Ausfälle oder Störungen sind, die ihre Funktionsfähigkeit und Versorgungssicherheit gefährden.

Um Vulnerabilität besser fassen zu können, ist es zweckmäßig, ihre Eigenschaften näher zu spezifizieren.

Vulnerabilität besitzt folgende Merkmale (vgl. Lenz 2009, S. 29ff). Sie ist:

Eigenschaften von Vulnerabilität

- *Objektbezogen:* Vulnerabilität bezieht sich auf ein bestimmtes Risikoelement und seinen (räumlichen und strukturellen) Kontext und resultiert aus den Eigenschaften des Risikoelements (z. B. resultiert die Vulnerabilität einer Wasserleitung u. a. aus der Beschaffenheit einer Dichtung. Eine kaputte Dichtung erhöht die Vulnerabilität). Risikoelemente können einzelne KI-Teile ebenso sein wie Subsysteme, Menschen oder Objekte, die in irgendeiner Form in die KI eingebunden sind.
- *Gefahrenspezifisch:* D. h. sie wird deutlich, wenn ein schädigendes Ereignis eintritt, das eine Auswirkung hat (z. B. physische Schäden). Vulnerabilität ist daher nicht per se feststellbar sondern steht immer in Bezug zu einem schädigenden Ereignis in einem bestimmten Ausmaß.
- *Immanent:* Vulnerabilität ist unabhängig davon gegeben, ob eine Gefahr tatsächlich besteht. (z. B. ist ein Mensch, der nicht schwimmen kann, grundsätzlich gefährdet, in tiefem Gewässer zu ertrinken. Allerdings lässt sich dieses Risiko durch Meiden solcher Gewässer leicht minimieren. Die Vulnerabilität ist aber dennoch gegeben.)
- *Multidimensional:* eine Reihe von miteinander verwobenen Faktoren (etwa ökonomische, soziale, physische und Umwelt-Faktoren) beeinflussen das Ausmaß von Vulnerabilität.
- *Dynamisch:* Vulnerabilität ist keine statische Eigenschaft, sondern ein Zustand, der sich im Lauf der Zeit, durch Änderungen der Umweltfaktoren des Systems verändern kann (z. B. Hochwasser, dessen Ausmaß höher ist, als der Hochwasserschutz vorsieht, erhöht die Vulnerabilität).
- *Skalenbezogen:* Die Einflussfaktoren der Vulnerabilität können mit der (räumlichen) Skala der Betrachtung unterschiedlich sein. Etwa ist die Vulnerabilität eines gesamten Infrastruktur-Bereichs von anderen Faktoren abhängig als jene einer einzelnen Komponente. Deshalb ist es sinnvoll, unterschiedliche Betrachtungsebenen (z. B. national, regional, lokal) zu verwenden.

2.2 Vulnerabilität und Bewältigungskapazität

Inwieweit das Risiko eines Ausfalls kritischer Infrastruktur reduzierbar bzw. bewältigbar ist, hängt einerseits von der Vulnerabilität ab. Sie ist ein zentrales Kriterium zur Ermittlung, inwieweit ein Ereignis bzw. ein Störfall zu Beeinträchtigungen oder Ausfall kritischer Infrastruktur führen kann. Eine Reduktion der Vulnerabilität trägt somit dazu bei, Ausfallrisiken zu reduzieren. Ein weiterer relevanter Faktor ist die Bewältigungskapazität. Sie ist entscheidend, um die Funktionsfähigkeit bei einem Ausfall wieder herstellen zu können (Birkmann et al 2010). Zum besseren Schutz kritischer Infrastrukturen sind (unter vorausgesetztem Problembewusstsein) daher neben Maßnahmen zur Verringerung der Vulnerabilität auch Maßnahmen zur Erhöhung der Bewältigungskapazität erforderlich. Das umfasst insbe-

sondere Maßnahmen des Krisenmanagements (siehe Abschnitt 5). Um Vulnerabilität und Bewältigungskapazität besser fassbar zu machen, können verschiedene (miteinander verbundene) Indikatoren herangezogen werden (vgl. Lenz 2009, 51ff):

Indikatoren für Vulnerabilität

- *Robustheit:* Fähigkeit einer kritischen Infrastruktur, trotz physischer Einwirkung eines schädigenden Ereignisses funktionsfähig zu bleiben (ohne Einsatz von Notressourcen). Die Robustheit hängt u. a. von der Intensität, Art und Dauer des Ereignisses ab.
- *Pufferkapazität:* Fähigkeit, die Einwirkung eines schädigenden Ereignisses über einen bestimmten Zeitraum zu kompensieren. Pufferkapazität bezieht sich also auf die Dauer, die eine KI einem Ereignis standhält ohne in der Leistungserbringung beeinträchtigt zu werden.
- *Abhängigkeit:* Bezieht sich auf die Angewiesenheit der Funktionsfähigkeit einer KI an technische, organisatorische oder Umwelt-Bedingungen, wie andere Infrastrukturen (z. B. ein Computersystem ist auf die funktionierende Stromzufuhr angewiesen), organisatorische Gegebenheiten (z. B. Angewiesenheit auf Spezialpersonal) und umweltbedingte (z. B. Kühlwasserbedarf bei Kraftwerken etc.) Abhängigkeiten.
- *Anpassungsfähigkeit:* Die Funktionsfähigkeit kritischer Infrastrukturen unterliegt einer Reihe von Rahmenbedingungen (z. B. geographisch, ökonomisch, politisch, rechtlich etc.). Anpassungsfähigkeit bezieht sich auf die Fähigkeit der KI, bei sich verändernden Rahmenbedingungen funktionsfähig zu bleiben (z. B. Aufnahmelast bzw. Lastenmanagement des Stromnetzes).
- *Qualitätsniveau:* Bezieht sich auf den qualitativen Zustand der kritischen Infrastruktur. Hierbei sind insbesondere Pflege und Wartung relevant, um etwa Verschleiß und Abnutzung vorzubeugen.
- *Schutzniveau:* Bezieht sich darauf, inwieweit eine KI vor einer Gefahr geschützt ist (z. B. FI-Schalter).

Indikatoren für die Bewältigungskapazität

- *Bereitschaft:* Vorbereitungsgrad auf Störungen u. Ausfälle. Z. B. durch Krisen- und Notfallpläne, Sicherheitskonzepte, Personalschulungen, Notfallübungen und funktionsfähige Backup-Systeme.
- *Redundanz:* Mehrfaches Vorhandensein von Strukturen zur Erbringung derselben Leistung (z. B. parallel verlaufende Bahnstrecken, Backup-Systeme wie Notstrom-Aggregate).
- *Substituierbarkeit:* Ersetzbarkeit der Leistung einer kritischen Infrastruktur-Komponente durch eine andere Komponente bei einem Ausfall (also inwieweit lässt sich ein Ausfall durch alternative Leistungserbringung überbrücken?).
- *Transparenz:* Nachvollziehbarkeit des Aufbaus und der Funktionsweise der kritischen Infrastruktur.
- *Wiederherstellungsaufwand:* Der (zeitliche, personelle und finanzielle) Aufwand, um einen Ausfall zu bewältigen.

Es empfiehlt sich, diese Indikatoren bei Vulnerabilitätsanalysen von kritischen Infrastrukturen zu berücksichtigen. Um die Bewältigungskapazität auch bei unwahrscheinlichen, aber schwerwiegenden Ausfallrisiken (wie die im Kontext dieser Studie untersuchten) zu gewährleisten, gibt es eine Reihe von Herausforderungen, die in den Abschnitten 5.4 und vor allem 6 näher behandelt werden. Die folgenden Abschnitte befassen sich zunächst mit Ausfallrisiken und Einflussfaktoren.

3 Ausfallrisiken und Einflussfaktoren

Wie im vorherigen Abschnitt erläutert, umfasst Vulnerabilität im Kontext kritischer Infrastrukturen all jene Zustände, die die Anfälligkeit der Allgemeinheit für Gefahren erhöhen. Vulnerabilität ist naturgemäß eng verbunden mit dem Begriff Risiko, der allgemein die Wahrscheinlichkeit bezeichnet, dass ein ungewünschter Zustand aufgrund eines (schädigenden) Ereignisses erreicht wird (vgl. Renn 2008, Renn/Dreyer 2010), es also zu Schäden an bestimmten Schutzgütern kommt. Diese Eintrittswahrscheinlichkeit resultiert aus der Gefährdung, das Ausmaß des Schadens wird dagegen maßgeblich durch die Vulnerabilität bestimmt (Lenz 2009, 36).

Es existiert naturgemäß eine Fülle verschiedener Ausfallrisiken, im Folgenden werden hier nur exemplarisch einige angeführt (vgl. BBK 2006):

Ausfallrisiken

- Natur- und Umweltkatastrophen (Unwetter, Erdbeben, Überschwemmungen, Lawinen, Erdrutsche, Hitzewellen, Waldbrände, Extremwetter-Phänomene, etc.)
- Atomare Katastrophen
- Biologische Katastrophen (Epidemien, Pandemien, etc.)
- Chemische Katastrophen
- Datennetz-bezogene Gefahren
- E-Gefahren (Gefahren durch elektromagnetische Impulse)
- Gefahren durch die Freisetzung mechanischer und thermischer Energie
- Menschliches Versagen
- Gezielte Angriffe (z. B. durch Ausnützen technischer Schwachstellen, Sabotage, Cyber-Angriffe – Einsatz von Schad- und Spionagesoftware wie Trojanern, Viren, Würmern etc.)[14]
- Technisches Gebrechen, Materialschwäche, Überlastung, Systemfehler etc.

Eine Identifikation möglicher Risiken ist zwar hilfreich, um Sicherheitsvorkehrungen entwickeln zu können, die auch gegen spezifische Gefahren Schutz bieten können (für einige der angeführten Risiken existieren besondere Krisen- und Katastrophenschutzmaßnahmen, auf die hier nicht näher eingegangen wird). Allerdings lässt sich nicht jede potenzielle Gefahr bzw. jedes Risiko im Vorfeld bestimmen[15]. Um dieser Problematik zu begegnen

[14] Gezielte Angriffe auf IT-Systeme sind etwa ein zunehmendes Problem. Diese Problematik wird in Abschnitt 4.2 genauer behandelt.

[15] Dass die Frage, wodurch Infrastruktur zu kritischer Infrastruktur wird, keineswegs trivial ist, haben u. a. die im Rahmen dieser Studie durchgeführten Interviews und Diskussionen mit ExpertInnen gezeigt. Trotz teils sehr unterschiedlicher fachlicher Backgrounds herrschte unter den ExpertInnen weitgehend Konsens darüber, dass Kritikalität subjektiv ist und klassische Risikoanalysen nicht ausreichen, um mit den komplexen Bedrohungen moderner Infrastrukturen umgehen zu können.

erscheint ein vulnerabilitäts-orientierter Ansatz (wie in Abschnitt 2 skizziert) zweckmäßiger, wenngleich hier naturgemäß enge Zusammenhänge bestehen. Der wesentliche Mehrwert der Vulnerabilitäts-Orientierung liegt darin, dass sie Identifizierung und Einschätzung von Gefahren nicht nur auf vorab definierte externe Risikofaktoren begrenzt, sondern auch systemimmanente Aspekte berücksichtigen kann.

Wechselwirkungen und Exposition

Aus einer Meta-Ebene betrachtet, sind Wechselwirkungen zwischen einem KI-System und einem (potenziell) schädigenden Ereignis ein wichtiger Faktor, um ein mögliches Schadens- bzw. ein Ausfallrisiko abschätzen zu können. Präziser formuliert geht es hierbei um Exposition als wesentlichen Einflussfaktor. Basiskomponenten des Risikos sind nach Lenz Gefahr, Exposition und Vulnerabilität. Ein Zusammenspiel dieser drei Komponenten führt zu einem Ausfallrisiko. Die Exposition eines Risikoelements bezieht sich auf seine Einflussfaktoren wie etwa die räumliche Lage bzw. räumliche Nähe zu einer Gefahr (z. B. ein Kraftwerk, das sich in einer Erdbebenregion befindet, ist der Gefahr eines Erdbebens exponiert) (vgl. Lenz 2009, 39). Aus systemischer Perspektive lässt sich grob zwischen endogener und exogener Exposition unterscheiden. Endogen bezieht sich auf die Wechselwirkungen und potenziellen Risiken, die innerhalb des Meta-Systems kritischer Infrastruktur bestehen bzw. aus ihm selbst entstehen (z. B. durch Verschleißteile, defekte Schnittstellen udgl.). Exogen meint äußere Einwirkungen bzw. schädigende Ereignisse, die von außen auf das System einwirken (Blitzschlag). Diese Unterscheidung kann einerseits hilfreich sein, um jeweils gezieltere Maßnahmen zur Reduzierung von Risiken innerhalb und außerhalb eines KI-Systems entwickeln zu können (z. B. ein Blitzableiter ist eine Schutzmaßnahme gegen ein exogenes Risiko; ein FI-Schalter ist dagegen eine Maßnahme gegen ein endogenes Risiko (wenngleich es auch von außen ausgelöst werden kann). Andererseits verdeutlicht die Unterscheidung auch, dass eine klare Abgrenzung in der Praxis oftmals schwierig ist, insbesondere durch zunehmende Digitalisierung und Vernetzung, worauf in den folgenden Abschnitten noch näher eingegangen wird.

Endogene und exogene Exposition

Da die klassischen Risiken durch Naturkatastrophen etc. weitgehend bekannt sind, wird im Folgenden auf Risiken eingegangen, über deren Auswirkungen vergleichsweise weniger bekannt ist und die sich als elektromagnetische Phänomene auf Stromnetz und IKT auswirken können. Abschnitt 3.1 befasst sich mit Ausfallrisiken durch elektromagnetische Impulse (EMP). In Abschnitt 3.2 werden potenzielle Risiken durch das Phänomen Solarstürme diskutiert.

3.1 Ausfallrisiken durch elektromagnetische Pulse

Elektromagnetischer [Im]Puls [EMP]

Ein elektromagnetischer (Im)Puls (EMP) ist eine meist kurze, breitbandige elektromagnetische Strahlung, die sich auf elektrisch leitfähiges Material auswirken kann. Es kommt dabei zu einer sprunghaften Änderung einer elektrischen oder magnetischen Größe (z. B. der Stromstärke, Spannung, oder Feldstärke). Je nach Ausmaß kann ein EMP zu Störungen oder Beschädigungen elektronischer Geräte führen. Die Auswirkungen eines EMPs hängen von seinem Ausmaß ab. Hierbei sind die Anstiegszeit des Impulses und die maximale elektrische Feldstärke wesentliche Faktoren. Die Anstiegszeit ist die Zeitspanne zwischen „demjenigen Zeitpunkt, an dem der Impuls 10 % seines Maximalwertes erreicht hat bis zum Erreichen der 90 %-Marke. (…) Je kürzer die Anstiegszeit eines Impulses ist, umso stärker sind höher-frequente Anteile in ihm enthalten“ (Wolfsperger 2008, 468). Unterschiedliche Frequenzen können massive Störungen verursachen. Ein Impuls benötigt eine gewisse Energie in gespeicherter Form z. B. als geladener Kondensator, der dann durch eine Art Schaltvorgang schlagartig entladen wird. Auf diese Weise kann trotz begrenzter Energie eine sehr hohe Leistung erreicht werden. Grundsätzlich sind EMPs kein seltenes Phänomen und kommen in der Natur z. B. in Form von Blitzen[16] vor. Aber auch im Alltag treten EMPs auf: Beispielsweise entsteht schon beim Betätigen eines Lichtschalters ein leichter elektromagnetischer Impuls: Der Schalter schließt den Stromkreis und führt zu einem sprunghaften Stromanstieg, der aber i.d.R. keine spürbaren Auswirkungen hat. In größerem Rahmen (innerhalb eines Elektroenergiesystems wie dem Stromnetz) treten EMPs beim Schalten hoher Ströme auf, wodurch es an Induktivitäten wie etwa Transformatoren zu Spannungsspitzen bzw. Überspannungen kommt. Diese Impulse kommen aus dem System selbst und Netzbetreiber reduzieren die Auswirkungen z. B. durch Filterung (Wolfsperger 2008).

Anstiegszeit und elektrische Feldstärke

Abgesehen von diesen „routinemäßigen“ EMPs lassen sich folgende Arten unterscheiden:

Arten von EMP

- Blitze – LEMP – Lightning electromagnetic pulse
- Kernwaffendetonation – Nuklearer EMP (NEMP bzw. auch als HEMP – High altitude EMP bezeichnet)
- HPM – High Power Microwave
- EMP durch Solar-/Magnetsturm

EMPs lassen sich auch künstlich erzeugen. Ein NEMP/HEMP tritt auf, wenn Kernwaffen in großer Höhe (40-400 km) gezündet werden.[17] Dabei wird Gammastrahlung in enorm hohem Ausmaß freigesetzt, wodurch Teilchen in der Atmosphäre ionisieren[18] und elektromagnetische Schockwel-

[16] Blitze werden auch als LEMP – Lightning electromagnetic pulse bezeichnet.

[17] Hier lässt sich noch zwischen Zündung in der Atmosphäre (Endo-NEMP) und im Weltraum also außerhalb der Atmosphäre (Exo-NEMP) unterscheiden.

[18] Hier tritt der sogenannte Compton-Effekt ein, bei dem sich die Wellenlänge der Teilchen (Photonen) vergrößert.

len mit einer Anstiegszeit von ca. 4 ns (Nano-Sekunden) auftreten. Es kommt zu Wechselwirkungen zwischen den geladenen Teilchen und dem Erdmagnetfeld bei der Strom induziert wird. Die Anstiegszeit ist meist deutlich kürzer als etwa bei einem LEMP. Daher bieten hier herkömmliche Blitzschutzeinrichtungen keinen zuverlässigen Schutz vor NEMPs (Wolfsperger 2008, 469f). Aufgrund der Distanz wären die Auswirkungen durch Hitzeblitz, Druckwelle und Radioaktivität auf der Erde eher gering. Die schädigenden Auswirkungen auf elektronische Infrastruktur können dagegen enorm hoch sein. Im Umkreis mehrerer hundert Kilometer kann es zu erheblichen Schäden kommen. Das geschieht durch elektrische Kopplung: die vom EMP erzeugte Strahlung wird von leitfähigem Material wie in Infrastrukturteilen, Geräten etc. empfangen (wie bei einer Antenne) und ohne Schutz kommt es so zu Überspannung. Militärische Geräte sind durch elektromagnetische Schirmung vor EMPs geschützt. Zivile Geräte und Anlagen sind dagegen i.d.R. nicht gesondert abgeschirmt (Wolfsperger 2008). Wie gravierend die Auswirkungen sind, hängt hier vor allem von der Stärke der Detonation ab. Beim Eintreten eines EMPs kann zwischen drei Komponenten E1, E2 und E3 unterschieden werden. Alle drei sind Pulse, allerdings mit unterschiedlicher Dauer und Spannung. E1 ist der Puls, der unmittelbar nach der Detonation mit hoher Geschwindigkeit (ca. 90 % der Lichtgeschwindigkeit) und Amplitude (also Spannung)[19] erfolgt und bis zu 1 Mikrosekunde (1.000 Nanosekunden) dauert. Auf E1 folgen weitere Pulse E2 und E3, die eine niedrigere Amplitude und Stärke aufweisen aber länger anhalten als E1. E2 hat eine Dauer von bis zu 1 Sekunde und ähnelt zum Teil einem Blitz (mit Stromstärken bis zu 20.000 Ampere). Er ist dementsprechend einfacher abzuwehren als etwa E1. E3 ist noch geringer ausgeprägt als E2 mit Frequenzen unter 1 Hertz, aber längerer Dauer zwischen 10 und 1.000 Sekunden. E3 weist Ähnlichkeiten mit einem geomagnetischen Sturm auf und vice versa (wie im nächsten Abschnitt 3.2 beschrieben). Vor allem E1 und E3 können negative Auswirkungen auf kritische Infrastrukturen und insbesondere auf das Stromnetz haben.

Elektronische Kontrollsysteme als Achillesferse des Stromversorgungsnetzes

Grundsätzlich anfällig (da sie den induzierten Strom aufnehmen) sind naturgemäß leitfähige Materialien wie Antennen, Eisenbahnschienen, Pipelines, Stromnetze etc. Angeschlossene Geräte können so Spannungen ausgesetzt werden, die zu erheblichen Störungen führen können (je nach Ausmaß, Beschaffenheit der Infrastruktur, Abschirmung usw. siehe Abschnitt 3.3). Ein problematischer Aspekt ist die erhöhte Vulnerabilität moderner elektronischer Bauteile gegenüber EMPs. Elektronische Kontrollsysteme sind gewissermaßen die Achillesferse des Stromversorgungsnetzes (vgl. Butt 2010, Foster et al 2008). Röhren-basierte Systeme der 1960er Jahre waren vergleichsweise wesentlich weniger anfällig als heutige integrierte Schaltkreise (Butt 2010). Speziell elektronische Geräte, die an lange Leitungen angeschlossen sind, sind besonders vulnerabel gegenüber EMP (E1 und E3).

[19] Bei E1 können rund 2 Millionen Elektronenvolt (MeV) entstehen.

Die Vulnerabilität eines Systems hängt grundsätzlich von der Beschaffenheit seiner Infrastruktur ab (siehe Abschnitt 3.3). Ein Aspekt ist die Länge der Leitung, grundsätzlich gilt: je länger die Leitung zwischen Leistungserzeuger (Stromquelle) und Verbraucher, desto mehr Energie kann aufgenommen werden, wodurch aber auch das Schadenspotenzial steigt. Wird hierbei neben dem „normalen" Stromfluss zusätzlicher Strom induziert durch einen EMP, kann es zu erheblicher Überspannung und letztlich zum Zusammenbruch des Systems oder Teilen davon führen. Diesbezüglich besonders anfällig sind etwa das Stromnetz und Leitungen im Telekommunikationsbereich (wie Telefon und Internet), sofern diese über längere Distanzen (über 100 Km) gehen (Butt 2010). Bezüglich Internet-Leitungen ist allerdings zu beachten, dass Glasfaserkabel nicht durch EMP gefährdet sind. Entgegen gängiger Meinungen wird nicht jede Art von elektronischem System grundsätzlich von einem EMP zerstört. Das hängt zum einen vom konkreten Ausmaß des Impulses ab. Zum anderen sind insbesondere kleinere, in sich geschlossene Systeme (wie etwa Fahrzeuge, Gebäude, tragbare Generatoren, Portables etc.), die nicht an längere Leitungen angeschlossen sind, weitaus weniger anfällig. Wenn hier Störungen auftreten, sind diese oftmals nur temporärer Natur, Bauteile werden also nicht per se zerstört (Baker 2015). Grundsätzlich bieten Faradaysche Käfige Schutz, Gebäude oder Fahrzeuge sind dementsprechend weniger gefährdet. Dem Stromnetz kommt besondere Bedeutung zu, da es als Basisinfrastruktur praktisch alle anderen kritischen Infrastruktursysteme versorgt. Die Folgewirkungen von Kaskadeneffekten durch Ausfälle der Stromversorgung können daher indirekt zu erheblichen Problemen führen, die in Folge auch weitere Infrastruktursysteme betreffen können (siehe Abschnitt 4). Eine Erhöhung des Schutzniveaus im Stromnetz (etwa durch Überspannungsschutz und elektromagnetische Schirmung) kann dementsprechend die Resilienz der kritischen Infrastruktur insgesamt verbessern (Baker 2015). Für das Setzen von Schutzmaßnahmen ist eine Reihe von Einflussfaktoren relevant, die in Abschnitt 3.3 näher erläutert werden.

HPM-Waffen erlauben gezielte Angriffe

Das Erzeugen eines NEMPs ist keineswegs trivial und erfordert nicht zuletzt den Einsatz erheblicher Mengen nuklearen Sprengstoffs und Trägerraketen (Butt 2010). Allerdings gibt es neben NEMPs auch spezielle Waffensysteme – sogenannte HPM-Waffen, die mit Mikrowellenstrahlung (High Power Microwave – HPM) arbeiten. Diese Waffen werden vor allem vom Militär entwickelt und eingesetzt (etwa von US-Truppen im Balkan und im Irakkrieg). Dennoch ist hier durch die (verglichen mit NEMPs) einfachere Beschaffung von einem neuen Bedrohungspotenzial auszugehen, wenn auch terroristische Gruppierungen derartige Waffen nutzen können. HPM-Waffen beinhalten EMP-Generatoren, die auf unterschiedliche Weise Impulse erzeugen können (mit Anstiegszeiten von 1 bis 4 Nanosekunden). Ultra-Wide-Band (UWB) Generatoren können sogar Impulse mit Anstiegszeiten unter 1 Nanosekunde erzeugen und strahlen Energie im Frequenzbereich zwischen 100 MHz und 1 GHz ab. Gerade in diesem Bereich sind elektronische Geräte oftmals besonders sensibel und können somit gezielt gestört werden. Es gibt auch HPM-Waffen, die laufend hochenergetische Störungen mit sinusförmigem Zeitverlauf hervorrufen. Diese Art vom

EMPs funktioniert primär in geringer Distanz und hat wesentlich weniger Breitenwirkung als ein NEMP (Wolfsperger 2008, 467ff). Das heißt die Gefahr von HPM-Waffen bezieht sich eher auf einzelne Anlagen und nicht auf großflächige Teile kritischer Infrastruktur. Allerdings lassen sich auf diese Weise Infrastruktursysteme mitunter gezielter stören.

NEMPs im Zeichen des Kalten Krieges

NEMP-Tests in den 1960er Jahren

Die oben angeführten EMPs entsprechen Waffen und waren vor allem zur Zeit des Kalten Krieges Gegenstand militärischer Forschung. Um die heutige Bedeutung von EMPs für den Schutz kritischer Infrastrukturen besser fassen zu können, ist auch der historische Hintergrund relevant. Es gibt insgesamt wenig empirische Befunde zu den Auswirkungen von NEMPs. Vor allem die USA und die UdSSR experimentierten in den 1960er Jahren auch mit dieser Form von Waffen. Insgesamt 20 derartige Tests wurden von beiden Supermächten durchgeführt. Bekannt ist etwa der Test „Starfish Prime“, bei dem die USA 1962 über der Hawaiianischen Insel Oahu im Pazifik eine Bombe mit 1,4 Megatonnen in der Höhe von ca. 400 km (250 Meilen) zündeten. Dabei wurde ein EMP erzeugt, der Stromleitungen, Straßenbeleuchtungen und Telefonleitungen beschädigt hat. Auch Russland hat ähnliche Tests durchgeführt. Beim sowjetischen „K-Projekt“ wurden über Kasachstan 1961 Tests mit 1,2 Kilotonnen Sprengstoff in einer Höhe von 150-300 km gezündet. Die Effekte auf die Infrastruktur waren hierbei eher gering. Bei einem weiteren „Test 184“ detonierte in 290 km Höhe 300 Kilotonnen Nuklearsprengstoff. Bei dieser Höhe beträgt der Detonationsradius bis zu 1900 Kilometer. Die Schäden waren dementsprechend hoch, u. a. wurden Überlandleitungen, Telefonleitungen und Diesel Generatoren beschädigt. Letztere traten als Folgewirkung nach der Detonation auf – es kam zu Defekten in der Isolierung, wodurch der Antrieb (die Spulen) der Generatoren beschädigt wurden (vgl. Butt 2010, Foster et al 2008). Diese dokumentierten Fälle liegen bereits einige Jahrzehnte zurück und in Anbetracht der rasanten technischen Entwicklung, insbesondere der Zunahme vernetzter Technologien, sind die damaligen Auswirkungen auf Infrastrukturen nur bedingt auf die heutige Zeit übertragbar. Der heute wesentlich höhere Vernetzungsgrad und die dementsprechend hohe Abhängigkeit der Gesellschaft von Infrastruktursystemen ermöglichen hierbei auch ein höheres Schadenspotenzial.

Revival der Forschung zu nuklearen EMPs nach 9/11

Nicht zuletzt durch die Terroranschläge vom 11. September 2001 auf das World Trade Center in New York kam es in den USA und weltweit zu einer Veränderung der Sicherheitspolitik wodurch auch potenzielle Gefahren durch NEMPs wieder an Bedeutung gewannen. In den USA wurde im Jahr 2001 eine eigene Expertenkommission (EMP Commission) eingerichtet, um zu untersuchen, inwieweit die Vereinigten Staaten durch EMPs bedroht sind (Spencer 2004). Dazu wurden auch Tests mit EMPs durchgeführt, um die Robustheit von Geräten zu untersuchen. Allerdings sind laut Butt (2010) wenig Details über das Ausmaß der erzeugten EMPs bekannt. Die EMP Kommission kam u. a. zu dem Schluss, dass nukleare EMPs ernsthafte Risiken für die USA bedeuten. Vor allem das US-Stromnetz und

zivile Telekommunikationsnetze könnten durch NEMPs beschädigt werden. Die grundsätzliche Verwundbarkeit kritischer Infrastrukturen durch EMPs wurde auch in einem jüngeren Bericht des US Government Accountability Office erneut festgestellt (GAO 2016). Eine Härtung ziviler Systeme in ihrer Gesamtheit ist kaum durchführbar, aber ggfs. unzureichend abgesicherte sensible militärische Geräte und strategisch wichtige Infrastrukturkomponenten sollten geschützt werden. Allerdings ist es schwierig zu beurteilen, welche Akteure tatsächlich in der Lage wären, einen NEMP Angriff durchzuführen. Die Befähigung dazu lag primär bei den Supermächten (vgl. Spencer 2004). Bei NEMP handelt es sich also letztlich um eine militärische Gefahr, die eine kriegerische Handlung voraussetzt. Dementsprechend ist dieses Szenario weniger eine technisches, sondern eher ein politisch-militärisches. Derartige Waffen sind aufwändig und teuer herzustellen. Neben den wirtschaftlichen Kosten ist es vor allem politisch kostspielig, denn es wäre eine kriegerische Handlung gegenüber dem Land, das vom NEMP betroffen ist. Die Erzeugung eines NEMP (eine bzw. mehrere Atomwaffen) erfordert enorme Ressourcen, über die i.d.R. nur militärische Akteure wie Staaten oder paramilitärische Organisationen verfügen. In einem weiteren Bericht kam die EMP Kommission u. a. zu dem Schluss (Foster et al 2008):

> *The consequences of an EMP event should be prepared for and protected against to the extent it is reasonably possible. Cold War-style deterrence through mutual assured destruction is not likely to be an effective threat against potential protagonists that are either failing states or trans-national groups. Therefore, making preparations to manage the effects of an EMP attack, including understanding what has happened, maintaining situational awareness, having plans in place to recover, challenging and exercising those plans, and reducing vulnerabilities, is critical to reducing the consequences, and thus probability, of attack. The appropriate national-level approach should balance prevention, protection, and recovery.*

Geringe Wahrscheinlichkeit für UK

Auch das britische Defence Committee des House of Commons hat sich mit der Thematik befasst. Hierbei wurde die Gefahr nuklearer EMPs aufgrund des potenziell hohen Schadensausmaßes zwar grundsätzlich als hoch eingestuft, die Wahrscheinlichkeit aber als gering (DC 2012). Das gilt insbesondere für Europa und Länder, die nicht in militärische Konflikte involviert sind. Wie bereits erläutert, setzt ein NEMP eine kriegerische Handlung voraus, die dementsprechend primär in den Zuständigkeitsbereich des Militärs fallen würde. Eine stringente Absicherung des gesamten zivilen Bereichs vor eventuellen künftigen Kriegszuständen erscheint aufgrund des hohen technischen, organisatorischen und finanziellen Aufwands schwer durchführbar. Zudem sind Gefahren dieser Art insbesondere Gegenstand internationaler (Außen-)Politik und Diplomatie. Hier sollte daher ggfs. ein Dialog zwischen Wissenschaft und Politik geführt werden, um genauer zu ermitteln inwieweit, bzw. in welchen Bereichen eine Absicherung notwendig und sinnvoll erscheint und unter welchen Rahmenbedingungen.

… und Österreich

3.2 Solarstürme

Ein besonderes Phänomen stellen sogenannte Solarstürme dar. Ein Sonnensturm entsteht durch Sonneneruption („Coronal Mass Ejection" – CME) bei der geladene Teilchen in Form von Plasmawolken aus der Sonne dringen. Das führt nicht unbedingt zu bedrohlichen Situationen, sondern mündet häufig im Naturschauspiel der Polarlichter (Aurora Borealis). Sonnenstürme bzw. geomagnetische Stürme sind auf erhöhte Sonnenaktivität zurückzuführen. Je mehr Sonnenflecken es auf der Sonne gibt, desto größer ist die Strahlungsaktivität der Sonne (vgl. Cannon et al 2013). Das bezieht sich nicht nur auf die Licht- und Wärmestrahlung sondern auch auf sogenannte Plasmaströme.[20] Bei der sogenannten Rekonnexion magnetischer Felder werden Magnetfeldkonfigurationen transformiert und die im Magnetfeld gespeicherte Energie wird in kinetische Energie der geladenen Teilchen umgewandelt. Dieses Phänomen tritt in sogenannten Plasmen auf. Das sind ionisierte Gase, die im Weltraum vor allem aus Protonen und Elektronen bestehen (Paschmann 2006). Das Auftreten von Sonnenflecken ist dynamisch, d. h. die Anzahl von Sonnenflecken verändert sich im Lauf der Zeit. Der Verlauf folgt dabei einem Zyklus wobei rund alle 11 Jahre die Anzahl der Sonnenflecke zunimmt. Abbildung 1 zeigt den Verlauf der sogenannten „Solar cylces" 23 und 24 von 1995 bis 2020. Wie der Kurvenverlauf zeigt, wurden in diesem Jahrtausend von der NASA insbesondere im Jahr 2001 und 2012 erhöhte Aktivitäten festgestellt. Auch 2015 ist ein Jahr mit erhöhter Solaraktivität, Anfang des Jahres kam es hier zu Sonnensturmphänomenen, die aber zu keinen spürbaren Auswirkungen auf der Erde führten (NASA 2015). Grundsätzlich kann es insbesondere nach einem Peak zu erhöhtem Plasmaausstoß kommen, in der Praxis gibt es aber immer wieder Abweichungen und unvorhergesehene Ereignisse (vgl. Möstl et al 2015).

Sonnenstürme als zyklisches Phänomen

[20] Der Sonnenwind bläst mit einer Geschwindigkeit von rund 350 km/s mit einer Dichte von ca. 6.6 Protonen pro cm³. Für aktuelles Wetter siehe etwa space-weather.com.

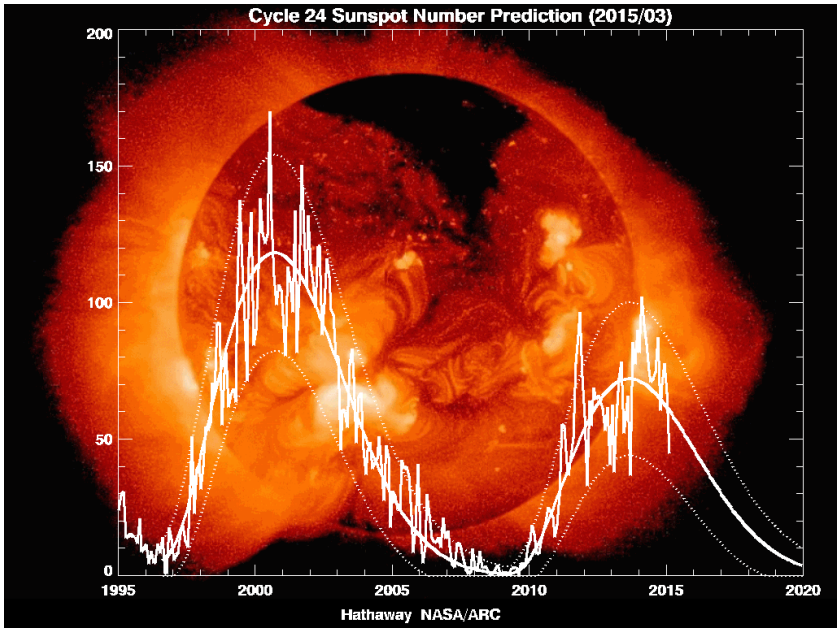

Abbildung 2: Solar-Cycles 23 und 24, Quelle: NASA[21]

Gefährlich werden kann ein starker Sonnensturm dann, wenn er oder eine Plasmawolke die Erdoberfläche trifft. Das Prinzip ist hier ähnlich wie bei einem EMP (insbesondere dem Typ E3). Das heißt es kommt zu einem elektromagnetischen Impuls, der auf das Erdmagnetfeld trifft. Es entsteht also ein geomagnetisch induzierter Strom und in Folge kann es zu Wechselwirkungen zwischen dem (externen) Magnetfeld der Plasmawolke und dem Erdmagnetfeld kommen.[22] Das kann zu Beeinträchtigungen erdnaher Systeme führen und je nach Ausmaß des Solarsturms können auch Systeme auf dem Boden betroffen sein. Die potenziellen Auswirkungen sind hierbei auch ähnlich wie bei einem E3 EMP, wobei das Ausmaß hier noch deutlich schwieriger abschätzbar ist. Grundsätzlich sind zunächst jene Systeme betroffen, die eine geringe Distanz zum auftretenden Magnetfeld haben, also primär Systeme über der Atmosphäre wie Satellitensysteme oder der Flugverkehr. In weiterer Folge können aber auch bodennahe Systeme betroffen sein. Gefährdet ist hier in erster Linie das Stromnetz, das mitunter enormen Impulsen von Gleichstrom ausgesetzt ist, die zu Überspannung und Beschädigung führen können. Ein elektromagnetischer Impuls führt dazu, dass Gleichstrom erzeugt wird. Da durch die Stromnetze Wechselstrom fließt, können diese nicht mit Gleichstrom umgehen, ab einer gewissen Stärke kommt es zu Spannungsstörungen, ähnlich wie bei einem Kurzschluss, und dadurch mitunter zur Beeinträchtigung oder Ausfall kritischer Infrastruktur-Komponenten, insbesondere von Transformatoren.

Gefahr vor allem für Satellitensysteme

[21] solarscience.msfc.nasa.gov/predict.shtml.

[22] Im Englischen ist das Phänomen daher auch bekannt als GMD (geomagnetic disturbances bzw. geomagnetische Störungen) oder GIC (geomagnetically induced currents) – geomagnetisch induzierte Ströme.

Unten stehende Grafik skizziert die potenzielle Vielfalt der Auswirkungen, über die aber bislang wenig faktisches Wissen existiert. Von den Auswirkungen können auch Telekommunikationsnetze betroffen sein. Bei enormem Ausmaß kann es mitunter auch zu erhöhter Korrosion in leitfähigen Materialien wie Ölpipelines, Bahngleisen, etc. kommen (DC 2012; Cannon et al 2013). Wichtig ist hierbei vor allem die Distanz zum Eintrittsereignis (der Stelle, wo die Magnetfeldwechselwirkungen auftreten). Nachdem das Ereignis (rund 200 km) außerhalb der Erdoberfläche (über der Atmosphäre) stattfindet, sind Effekte auf bodennahe Systeme extrem unwahrscheinlich. Primär betroffen sind all jene Systeme mit der geringsten Distanz, also Weltraumequipment wie Satelliten. Nur ein äußerst starker Sonnensturm kann potenziell auch Auswirkungen auf Bodensysteme haben. Bei Flugzeugen, die sich während eines Solarsturms in der Luft befinden, wären Passagiere und Crew erhöhter Strahlung ausgesetzt[23].

Figure 1: Impacts of space weather © L. J. Lanzerotti, Bell Laboratories, Lucent Technologies, Inc.

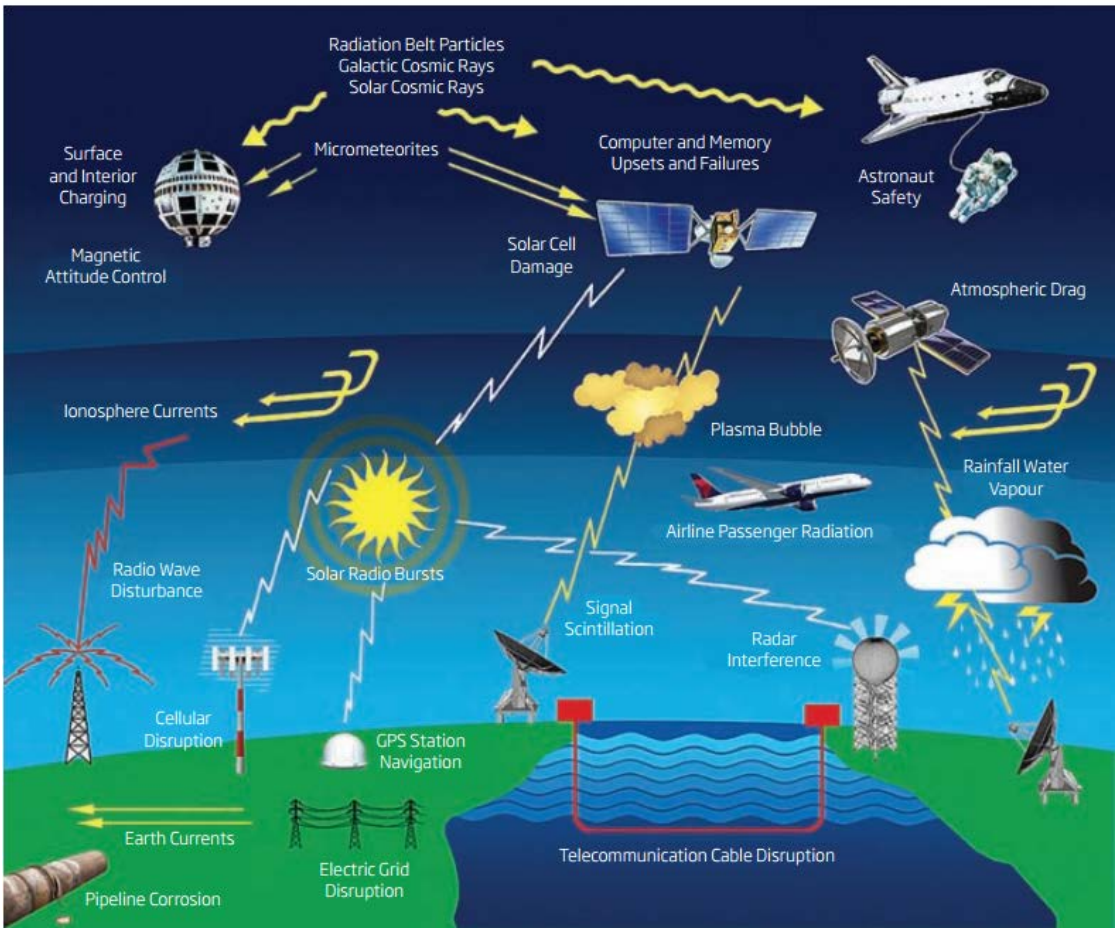

Abbildung 3: Übersicht zu möglichen Space Weather Impacts, Quelle: Cannon et al 2013

[23] Am 4. November 2015 wurden aufgrund geomagnetischer Strahlung Radarprobleme bei Schwedischen Flugzeugen beobachtet thewatchers.adorraeli.com/2015/11/05/the-sweden-case-aircrafts-disappear-from-radars-due-to-solar-storm/.

Es gibt zudem auch wenig empirische Befunde für Störfälle, die durch geomagnetische Sonnenaktivität verursacht wurden.[24] Die folgende Tabelle zeigt eine kurze Übersicht zu Vorfällen, bei denen es zu Störungen kam (vgl. Maynard/Smith/Gonzalez 2013; Piccinelli 2014, Krausmann 2014):

Tabelle 1: Übersicht zu dokumentierten Auswirkungen von Solarstürmen

Jahr	Ort	Ereignis
1806	Berlin, Deutschland	Von Humboldt dokumentierte Abweichungen der Kompassnadel in Berlin; auf die größte Störung folgend konnten Polarlichter in Berlin beobachtet werden.
1859	USA	Carrington-Event (benannt nach dem Wissenschafter, der es dokumentiert hat)
1921	New York, USA, Schweden	New York Railway Storm, Störungen und Ausfälle im Verkehrsleitsystem der Eisenbahn in NY, Störungen in Telegrafen- und Telefonnetzen, Brand einer schwedischen Telefonstation
1982	Schweden	Spannungsschwankungen im Verkehrsleitsystem der schwedischen Eisenbahn
1989	Quebec, Kanada	Beschädigung von Transformatoren und mehrstündige Stromausfälle
2003	Mehrere Teile der USA und Schweden	Sogenannter „Halloween Storm", mehrstündige Stromausfälle, Radarstörungen

Carrington-Event

Solarstürme sind schon lange dokumentiert. Bereits Alexander von Humboldt stellte während Polarlichterscheinungen Kompassschwankungen fest. Das sogenannte Carrington-Event bezieht sich auf ein Weltraumwetterereignis 1859, bei dem schwere Schäden im gerade entstehenden Telegrafennetz verursacht und Feuer in Telegrafenstationen entfacht wurden. Beim „Railway Storm" 1921 im Raum New York wurde das Eisenbahnnetz und Telefon- und Telegraphennetze massiv gestört; in Schweden kam es zu einem Brand in einer Telefonstation. Während eines Solarsturms am 14 Juli 1982 sind in Schweden Vorfälle dokumentiert, bei denen das Verkehrsleitsystem der Eisenbahn mit Spannungsschwankungen konfrontiert war. Es kam zu keinen Beschädigungen aber zu fehlerhaften Schaltungsvorgängen, wodurch sich Ampeln mehrfach eigenmächtig umschalteten (Wik et al 2009). 1989 fiel aufgrund eines schweren Sonnensturms die Stromversorgung von rund sechs Millionen Kanadiern im Großraum Montreal/ Quebec für mehrere Stunden aus. Auch der Kontakt zu zahlreichen Satelliten wurde unterbrochen. Im Jahr 2003 kam es durch einen Sonnensturm hoher Geschwindigkeit zu einem mehrstündigen Stromausfall in Schweden, einem Ausfall des europäischen Flugradars, zu Beeinträchtigungen des Flugverkehrs in den USA und zum Verlust des Forschungssatelliten „Midori 2".[25]

[24] Für eine Übersicht zu Weltraumwetterphänomenen siehe z. B. http://spaceweather.com.

[25] orf.at/stories/2130954/2130955/.

Auswirkungen von Solarstürmen

Carrington-Event als Worst Case Scenario

Das oben angeführte Carrington-Event wird häufig als Worst Case Scenario herangezogen, um auf die Gefahr eines weitreichenden Blackouts hinzuweisen. Allerdings lässt sich dieser Fall nur bedingt auf die heutige Zeit übertragen. Im Jahr 1859 war das Telegrafennetz eine wesentliche kritische Infrastruktur, ein Stromnetz existierte damals noch nicht und es war noch wenig über Isolierung, Abschirmung und dergleichen bekannt. Seit dem 19. Jahrhundert hat sich ein enormer technischer Wandel vollzogen und heutige Infrastrukturen sind daher kaum mit jenen von damals vergleichbar. Geomagnetische Ströme sind insofern heute besonders relevant, da sie ein höheres Schadenspotenzial auf moderne kritische Infrastruktursysteme bedeuten können, deren Funktionsfähigkeit wesentlich von der Stromversorgung abhängt. Schätzungen zufolge könnten bei einem Magnetsturm wie er 1921 auftrat aus heutiger Sicht bis zu 130 Mio. Menschen in den USA von der Stromversorgung abgeschnitten werden und bis zu 350 Transformatoren erheblich beschädigt werden (NRC 2008). Es lassen sich jedoch nur bedingt Rückschlüsse auf andere Länder ziehen, da die Netzstruktur in jedem Land unterschiedlich ist. Und die USA teilweise durch die geographische Lage in Nähe des Nordpols (siehe Abschnitt 3.3) einem deutlich höheren Risiko ausgesetzt sind. So wird das Risiko in Großbritannien bei Eintreten eines Sonnensturms als moderat aber aufgrund der anderen Beschaffenheit des Stromnetzes im Vergleich zu den USA als geringer eingeschätzt. Die Unberechenbarkeit des Weltraumwetters wird allerdings als generelles Problem betrachtet, das genauerer Analyse der potenziellen Folgen bedarf, insbesondere für Stromnetz und Satellitensysteme (DC 2012, Cannon et al 2013). Simulationen bezüglich der Auswirkungen eines mit dem Carrington-Event vergleichbaren Sturms auf das Stromnetz zeigen u. a., dass die induzierten Ströme sehr schnell zur Erhitzung und Überhitzung einzelner Komponenten (insbesondere Bindebleche und Spulen) führen können (Maynard/Smith/Gonzalez 2013). Der UK Royal Academy of Engineering zufolge könnte ein Super-Solarsturm vergleichbar mit Carrington zu Schäden bei bis zu sieben Hochspannungs-Transformatoren in England, Wales und Schottland führen. Reparaturen könnten mehrere Wochen und Monate dauern. Vom Ausfall bis zum Normalbetrieb könnten lt. DC (2012) zwei bis drei Monate vergehen. Da es bei den meisten Knotenpunkten mehr als nur einen Transformator gibt, würden allerdings nicht alle Schäden notwendigerweise zu einer Versorgungsunterbrechung führen. Allerdings könnten zumindest zwei Knotenpunkte völlig ausfallen (Cannon et al 2013). Für Österreich sind hier bislang keine gesonderten Daten bekannt, es ist aber davon auszugehen, dass Beschädigungen von Transformatoren ähnliche Auswirkungen hätten. Auf EU-Ebene wurde 2013 ein Workshop mit Vertretern europäischer und amerikanischer Stromnetzbetreiber abgehalten, um die Problematik zu beleuchten und Erfahrungen auszutauschen. Unter anderem wurde festgestellt, dass noch zu wenig über die Effekte von Weltraumwetterphänomenen auf das Stromnetz bekannt ist und insbesondere Interdependenzen zwischen kritischen Infrastrukturen bislang nicht berücksichtigt wurden.

Auswirkungen auf heutige Netze unklar

Dadurch können weitere Vulnerabilitäten entstehen, wie etwa durch die Anbindung von GPS und anderen Satelliten-Systemen in der Energieversorgung (Krausmann et al 2013).

Solarstürme eher unwahrscheinlich aber mit potentiell hohem Schadensausmaß

Grundsätzlich sind Auswirkungen durch Solarstürme auf der Erde eher unwahrscheinlich (vgl. Maynard/Smith/Gonzalez 2013; Cannon et al 2013). Problematisch ist allerdings, dass es bei Auftreffen eines starken Ereignisses auf das Erdmagnetfeld zu erheblichen Auswirkungen kommen kann, die sehr schwer abschätzbar sind. Vieles über Sonneneruptionen und Solarstürme ist bislang noch unerforscht. Auch der vergleichsweise kurze Beobachtungszeitraum stellt ein Problem dar (ca. 160 Jahre wissenschaftliche Beobachtung vs. 4,5 Milliarden Jahre Alter der Sonne). Das Weltraumwetter wird laufend beobachtet und es werden regelmäßig Prognosen über die Sonnenaktivität erstellt. Neben der NASA[26] und anderen Weltraumforschungseinrichtungen befassen sich auch meteorologische Institute wie etwa die österreichische Zentralanstalt für Meteorologie und Geodynamik (ZAMG) und das Institut für Weltraumforschung der ÖAW mit geomagnetischer Aktivität und stellen laufend eine Reihe von Messdaten und Informationen bereit.[27] Diese Informationen sind von hoher Bedeutung für die Weltraumforschung, Satellitensysteme und den Flugverkehr. Es dauert rund einen bis drei Tage, bis eine solare Plasmawolke auf die Erde trifft. Innerhalb von ca. sechs Stunden kann die ungefähre Zeit des Auftreffens auf die Erde prognostiziert werden (UK Gov 2015). Wird eine Plasmawolke von kritischem Ausmaß gesichtet (ab 200 Nanotesla), werden ggfs. Behörden und Netzbetreiber informiert. Die Entwicklung eines Frühwarnsystems ist derzeit Teil eines Forschungsprojektes von ZAMG und APG.

Beobachtung der Sonnenaktivität und Frühwarnung

Trotz dieser laufenden Beobachtungen kommt es immer wieder zu unvorhergesehenem Verhalten. So wurde etwa für 2014 prognostiziert, dass ein starker Sonnensturm die Erde mit dementsprechend hohen Auswirkungen träfe. Dieser Sturm steuerte zwar auf die Erde zu, änderte dann aber unerwartet seine Richtung, zog vorbei und es kam letztlich zu keinen Wechselwirkungen (Möstl et al 2015).[28] Die Ursache lag in starken Magnetfeldern nahe der Quellregion auf der Sonne, wodurch es zur Richtungsänderung des Sonnensturms kam. Es gibt daher erheblichen Bedarf nach weiterer Forschung und der Entwicklung von wirksameren Frühwarnsystemen und Forecasting, um die Unberechenbarkeit des Weltraumwetters zu reduzieren[29] und bessere Vorsorgemaßnahmen entwickeln zu können (vgl. DC 2012, Cannon et al 2013, Möstl et al 2015). Auch über die tatsächlich möglichen Auswirkungen auf der Erde ist relativ wenig bekannt. Es besteht daher in diesem Bereich weiterer Forschungsbedarf, insbesondere auch hinsichtlich der Bedeutung von Solarstürmen für Vernetzung und Systemabhängigkeiten.

Forschungsbedarf

[26] Siehe z. B. spaceweather.com.

[27] conrad-observatory.at/cmsjoomla/de/magnetik-ueberblick/geomagnetic-activity.

[28] science.orf.at/stories/1759277.

[29] Laut Baker (2015) sollten hier vor allem die Zeitspannen der Satelliteninformation (15-45 Min.) verringert werden, um frühzeitig aktuelle Information zu erhalten.

3.3 Einflussfaktoren

Die in den vorigen Abschnitten beschriebenen Gefahren durch verschiedene Arten von EMPs und deren Auswirkungen hängen von einer Reihe miteinander verbundener physischer und technologischer Einflussfaktoren ab. Dazu zählen insbesondere (vgl. Maynard/Smith/Gonzalez 2013; Cannon et al 2013):

Ausmaß und Stärke

- *Ausmaß und Stärke* des EMP bzw. Solarsturms.

Beschaffenheit der Infrastruktur

- *Die Beschaffenheit der Infrastruktur:* Beim Stromnetz als zentrale Infrastruktur sind hier vor allem relevant: Länge der Übertragungsleitung, Kilovolt Leistung, Widerstandsfähigkeit der Hochspannungstransformatoren, Bauweise und Kernkonstruktion der Transformatoren, Vorhandensein von Kondensatoren zur Abschirmung elektromagnetischer Strahlung. Glasfaserkabel sind durch EMPs nicht verwundbar, allerdings können angeschlossene elektronische Bauteile durch EMPs gestört werden (Spencer 2004, Butt 2010). Hochfrequenz-Kommunikation (wie etwa Funksysteme, Hör- und Rundfunk) ist weniger anfällig für Störungen (vgl. Cannon 2013, 6).

Netzstruktur

- *Netzstruktur, Leitungslänge und Aufnahmefähigkeit:* hierbei sind insbesondere drei Faktoren relevant: der Widerstand der Übertragungsleitung, der interne Widerstand und der Erdungswiderstand des Transformators. Die beiden letzten sind jeweils feste Größen während der Leitungswiderstand mit der Distanz zunimmt, zudem auch die Spannung: Je länger die Leitung desto größer die Spannung, wodurch insgesamt das Risiko mit der Pfadlänge zunimmt. Lange Überlandleitungen sind daher anfälliger.

Leitfähigkeit des Untergrunds

- *Leitfähigkeit und Beschaffenheit des Untergrunds:* Bei hoher Leitfähigkeit des Bodens kann der Strom eher leichter abgeleitet werden. Bei geringer Leitfähigkeit (wie etwa in gebirgigen Regionen) kann die Aufnahmefähigkeit des Netzes stärker belastet werden. Ein spezieller Aspekt ist der sog. „coastal effect“: Salzwasser ist sehr leitfähig. Allerdings können hier mitunter stärkere elektrische Felder entstehen. D. h. in küstennahen Regionen können hier noch komplexere Phänomene entstehen.

Art der Transformatoren

- *Beschaffenheit der Transformatoren als kritische Knotenpunkte:* einphasige Transformatoren sind anfälliger für Störungen durch geomagnetisch induzierten Strom als etwa dreiphasige Transformatoren.

Geographische Lage

- *Geographische Position und Breitenabhängigkeit:* Insbesondere bei Solarstürmen ist auch die Erdposition relevant. Ein Auftreffen einer Plasmawolke auf das Erdmagnetfeld ist äußert schwierig vorherzusehen. Induzierte Ströme treten idR. eher in Regionen hoher geografischer Breite auf und in der Nähe der Erdmagnetpole (wie USA, Kanada, Skandinavien, etc. sind grundsätzlich eher betroffen). Allerdings sind andere Länder nicht völlig außer Gefahr, wie Störfälle in Südafrika belegen[30].

[30] Sturzenegger (2014).

- *Abschirmung und elektromagnetische Verträglichkeit* (EMV), Robustheit von Satellitensystemen und Alternativen (z. B. bodennahe Redundanzen für Navigation, Zeitsynchronisation).

EMV Verträglichkeit

Durch das komplexe Zusammenspiel der verschiedenen Faktoren können Risiken für kritische Infrastrukturen entstehen. Über die genaue Wirkungsweise ist jedoch wenig bekannt, sowohl bezüglich einzelner Faktoren als auch deren Zusammenhänge. Das Risikopotenzial von geomagnetischen Stürmen auf kritische Infrastrukturen hängt nicht zuletzt wesentlich vom (in Abschnitt 3) erwähnten Faktor der Exposition ab, der hier mehrfache Dimensionen aufweist, die sich aus den verschiedenen Faktoren ergeben. Einerseits die räumliche Position von Erdmagnetfeld und Plasmawolke, die geografische Lage, die Leitfähigkeit des betroffenen Systems (wie viel Strom kann aufgenommen bzw. abgeleitet werden), Netzbeschaffenheit, etc.

Abschirmung möglich

Abschirmung gegen elektromagnetische Felder und EMPs ist prinzipiell möglich. Militärisches Gerät ist i.d.R. entsprechend abgeschirmt. Satelliten und anderes Weltraumequipment sind grundsätzlich ähnlich wie militärische Geräte gehärtet und vor elektromagnetischer Strahlung abgeschirmt. Dennoch treten auch hier manchmal Störungen auf. Im Jahr 2012 kam es etwa zu solchen Beeinträchtigungen und einer kurzfristigen Störung der Raumsonde Venus Express[31]. Schutzmaßnahmen sind etwa die sogenannte Galvanische Entkopplung, bei der eine elektrische Leitung zwischen Stromkreisen vermieden wird, die aber miteinander verzahnt sind (etwa im gleichen Gehäuse oder Teil der gleichen Funktionseinheit sind und wechselseitig Leistung austauschen. Auch Faradaysche Käfige bieten grundsätzlich Schutz. Diese und andere Schutzvorkehrungen sind Gegenstand elektromagnetischer Verträglichkeit (EMV), die die Abschirmung gegen elektromagnetische Strahlung in und zwischen Geräten bezweckt. Für die elektromagnetische Verträglichkeit gibt es eigene EMV Standards, die unterschiedliche Abschirmmöglichkeiten vorsehen. Relevante Normen zum Schutz vor EMP sind etwa DIN EN 61000-2-9 96, DIN EN 61000-2-10 99 oder DIN EN 61000-4-23. (vgl. Wolfsperger 2008). Dabei ist auch Schutz vor HPM-Waffen möglich, etwa durch Gebäudedämpfung. Elektromagnetische Wellen werden auch durch Gebäude selbst gedämpft, allerdings nur im Bereich von ca. 20 dB. Da die angenommene Feldstärke von HPM-Waffen ca. 100 KV/m beträgt und informationstechnische Geräte i.d.R. nur eine Störfestigkeit von rund 10 V/m aufweisen, ist „eine Dämpfung der Feldstärke um den Faktor 10.000 also 80 dB erforderlich (…). Diese Dämpfung sollte im Frequenzbereich 100 kHz – 4 GHz vorhanden sein, um alle Bedrohungsszenarien abzudecken“ (Wolfsperger 2008, 472). Zudem ist zu beachten, dass die Feldstärke mit der Entfernung abnimmt. Das heisst, auch organisatorische Maßnahmen können verhindern, dass etwa Angreifer in die räumliche Nähe eines Ziels (z. B. ein Kraftwerk) gelangen. Ein Bereich von einigen 100 m kann etwa erheblichen Schutz bieten. Die genaue Größe eines solchen organisatorischen Schutzbereichs

[31] spiegel.de/wissenschaft/natur/kosmische-eruption-sonnensturm-flaut-ohne-groessere-stoerungen-ab-a-820234.html.

kann nicht pauschal definiert werden, sondern hängt vom Bedrohungsausmaß ab. Die Stromversorgung kann neben elektromagnetischer Schirmdämpfung (z. B. nach dem IEEE-Standard 299) auch durch Einsatz von speziellen Filtern vor Überspannung geschützt werden (ebd.).

4 Systemabhängigkeiten und mögliche Kaskadeneffekte

Ein generelles Merkmal kritischer Infrastrukturen sind ihre komplexen Strukturen, die an eine Reihe gesellschaftlicher Bereiche gekoppelt sind. KI lassen sich in ihrer Gesamtheit als komplexes System begreifen, das aus einer Reihe von Elementen und Subsystemen mit zahlreichen Wechselwirkungen und Abhängigkeiten besteht (vgl. Lenz 2009). Klassische, homogene Netzinfrastrukturen sind heute weitgehend auch mit anderen Netzen verbunden. Insofern spielen Vernetzung bzw. Konnektivität eine zentrale Rolle für den Schutz kritischer Infrastrukturen. Ein Schadensereignis in einem stark vernetzten System kann sich rasch zu einer komplexen Schadenslage entwickeln und Kaskadeneffekte, also eine Kette von Ereignissen auslösen, die zum Totalausfall führen können; nicht zuletzt aufgrund des wachsenden Durchdringungsgrads mit IKT. Die Vernetzung zeichnet hier ein ambivalentes Bild: einerseits bringt sie wesentliche Vorteile mit sich, etwa begünstigen vernetzte Systeme die gesellschaftliche Grundversorgung (insbesondere mit Energie und Information). Andererseits erhöht die Vernetzung die Komplexität kritischer Infrastrukturen, wodurch auch die Anfälligkeit für Ausfallrisiken zunehmen kann. Einst physisch und logisch voneinander getrennte Systeme sind zunehmend miteinander verzahnt und so können Abhängigkeiten entstehen, die Anfälligkeit von Störungen und die Vulnerabilität erhöhen. Die dunklen Seiten der Vernetzung und Hyperkonnektivität werden auch im Global Risk Report 2015 des World Economic Forum als eine der zentralen Herausforderungen der Gesellschaft identifiziert (WEF 2015).

Vernetzung und Hyperkonnektivität als zentrale Herausforderung

Ein prominentes historisches Beispiel für gesellschaftliche Herausforderung der digitalen Vernetzung ist der sogenannte Millennium-Bug bzw. Jahr-2000-Problem[32]: Ursache des Problems war die fehleranfällige Verarbeitung von Jahreszahlen reduziert auf die jeweils letzten beiden Ziffern (z. B. 90 statt 1990) in Computersystemen. Vor allem in den 1960er und 1970er Jahren wurde dies oftmals gemacht, um die damals noch knapperen Speicherkapazitäten besser ausschöpfen zu können. Nicht berücksichtigt wurde, dass so Jahreszahlen wie 2000 und folgende nicht mehr korrekt darstellbar sein könnten und es in Folge weltweit zu zahlreichen Fehlberechnungen in Computersystemen kommen könnte. Im Jahr 1999 wurde medial verstärkt mit diversen Katastrophen-Szenarien vor dem Problem gewarnt. Im öffentlichen und privaten Sektor wurden Überprüfungen der Computersysteme durchgeführt und Maßnahmen gesetzt (etwa Komponenten erneuert, manche Banken deaktivierten zu Jahreswechsel prophylaktisch ihre Geldautomaten etc.). Letztlich kam es weltweit nur in geringem Ausmaß zu Störungen (z. B. Ausfall von Kreditkartentransaktionen in Großbritannien, fehlerhaft datierte Rechnungen in Italien, Ausfall von

Millennium-Bug als historisches Beispiel

[32] de.wikipedia.org/wiki/Jahr-2000-Problem.

Spielautomaten in den USA) und der Millennium-Bug verursachte keine global schwerwiegenderen Probleme. Dieses Beispiel verdeutlicht einige Schwierigkeiten: die mit Digitalisierung einhergehende hohe Komplexität erschwert eine Identifikation der tatsächlich gegebenen Schwachstellen und damit auch deren Beseitigung. Im Falle des Millennium-Bugs ist im Nachhinein schwer feststellbar, ob die Maßnahmen sinnvoll und effektiv waren oder das Problem übertrieben.

Systemperspektive als Analysetool

Um die Auswirkungen der Vernetzung besser betrachten zu können, erweist sich eine System-Perspektive als sinnvoll. Die folgende Abbildung skizziert einige Grundmerkmale von Systemen. Relevant ist hier vor allem die Unterscheidung zwischen dem System, seiner Umwelt und Schnittstellen, die als „Brücke“ unterschiedlicher Systeme fungieren. Hieraus können externe Abhängigkeiten entstehen, die Ausfallrisiken begünstigen können. Externe Abhängigkeiten sind insofern relevant, als sie etwa von Systembetreibern kritischer Infrastrukturen nicht, oder nur eingeschränkt kontrolliert werden können. Daraus resultiert ein besonderer Schutzbedarf für Schnittstellen.

Zur Erkenntnis, dass ein System mehr ist, als die Summe seiner einzelnen Teile, gelangte bereits Aristoteles und ebnete den Weg für das Verständnis komplexer Systeme, deren Eigenschaften sich nicht alleine anhand seiner Einzelkomponenten erfassen lassen. Wechselwirkungen zwischen den Systemelementen sowie dem System und seiner Umwelt spielen hierbei eine zentrale Rolle wie die folgende Abbildung skizziert.

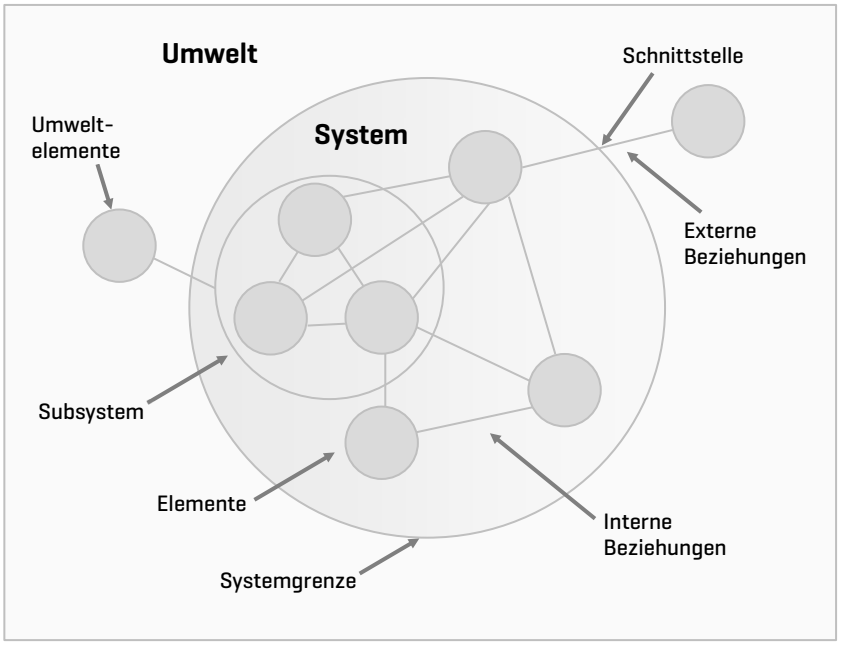

Abbildung 4: Systemperspektive und Grundbegriffe
Quelle: nach Schulte-Zurhausen 2002, S. 34

Die Systemperspektive bietet eine Heuristik, um von unterschiedlichen Ebenen zu untersuchen, welche Abhängigkeiten in und zwischen Systemen sowie externen Umwelteinflüssen bestehen. Etwa lässt sich das Stromnetz als kritisches Infrastruktur-System fassen, in dem insbesondere Transformatoren kritische Elemente darstellen, von denen etwa die Netzstruktur abhängig ist. Wenn Transformatoren mit anderen Systemen (etwa IT-Steuerung von Umspannwerken) interagieren, besteht eine gewisse Abhängigkeit zwischen dem Stromnetz zu diesen Systemen. Umweltfaktoren sind beispielsweise die in Kapitel 3 erwähnten Risiken. Zum Teil bestehen Abhängigkeiten zu externen Systemen im Bereich der Informations- und Kommunikationstechnologien. In einer Systemperspektive können Subsysteme differenziert (z. B. Internet, Mobilfunk und Telekommunikation, Satellitenbasierte Steuerung, etc.) und leichter analysiert werden. Diese Differenzierung kann es erleichtern, gezielte Abhängigkeiten und Wechselwirkungen in einem kritischen Infrastruktur-System bzw. einzelner Subsysteme zu identifizieren ohne immer das Gesamtsystem in seiner gesamten Komplexität berücksichtigen zu müssen. Das erscheint nicht zuletzt zweckmäßig, um die mit der Vernetzung einhergehende steigende Komplexität zu abstrahieren und logisch besser beherrschen zu können.

Differenzierung in Subsysteme zur leichteren Aufdeckung von Abhängigkeiten

Wie in Abschnitt 2.2 angeführt, beinträchtigen Abhängigkeiten die Funktionsfähigkeit kritischer Infrastruktur. Es gibt verschiedene Formen von Abhängigkeiten und Möglichkeiten, diese zu strukturieren etwa (vgl. Lenz 2009):

Formen von Abhängigkeiten

- *Physische Abhängigkeit:* ein typisches Beispiel ist die Stromversorgung, von der als Querschnittsinfrastruktur praktisch alle anderen Bereiche abhängig sind.
- *Geographische bzw. räumliche Abhängigkeit:* Systeme, die sich durch ihre räumliche Nähe wechselseitig beeinflussen können. Z. B. Eisenbahnbrücke, die über eine Autobahn führt; oder IT-Komponenten, die automatisiert Regelungsmechanismen steuern etc.
- *Umwelt-Abhängigkeit:* Umweltbedingungen wie Außentemperatur, Bodenbeschaffenheit, Witterungsschutz, Wasserversorgung (etwa zur Kühlung von Anlagen) etc.
- *Organisatorische bzw. Ressourcen-Abhängigkeit:* Der Betrieb kritischer Infrastrukturen benötigt bestimmte materielle und personelle Ressourcen wie Fachpersonal (z. B. Systemtechniker etc.), Energie (vor allem Strom), Treibstoff (z. B. Diesel, etwa auch zum Betrieb von Notstromaggregaten) etc.
- *Informations- und kommunikationstechnische Abhängigkeit:* Vor dem Hintergrund zunehmender Digitalisierung und Vernetzung kommt es hier zu neuartigen Formen der logischen bzw. virtuellen Abhängigkeit. Ähnlich wie das Stromnetz kommt heute IKT in praktisch allen Gesellschaftsbereichen zum Einsatz. Eine solche Abhängigkeit besteht insbesondere, wenn IKT für die Funktionsfähigkeit einer kritischen Infrastruktur benötigt wird und ein IKT-Ausfall diese erheblich beeinträchtigt. Das ist etwa bei Steuerungssystemen im Stromnetz oder in Verkehrsleitsystemen der Fall. Aber auch im Krisenfall können derartige Abhängigkeiten zum Problem werden, wenn etwa Krisenkommunikation nicht mehr möglich ist.

Die folgenden Abschnitte befassen sich eingehender mit der Abhängigkeitsproblematik. 4.1 geht auf einen Zusammenbruch des Stromnetzes ein und skizziert kurz einige der gesellschaftlichen Folgen. 4.2 beleuchtet exemplarisch wichtige Aspekte Informations- und kommunikationstechnischer Abhängigkeiten.

4.1 Blackout

Der Ausfall der Stromversorgung beeinträchtigt nicht nur sämtliche kritischen Infrastrukturen, die auf die Energieversorgung angewiesen sind, sondern unmittelbar auch alle BürgerInnen, wodurch sich zusätzliche Bedrohungen für die Gesellschaft ergeben.

Mögliche Gründe für Blackouts

Bei einem Blackout führt ein Störfall zum Zusammenbruch des Stromnetzes. Entweder wird das Übertragungsnetz selbst beschädigt, oder es kommt durch Ausfall eines Produzenten[33] zu einem plötzlichen Spannungsabfall. Auch zu hohe Einspeisung in Regionen mit hoher dezentraler Erzeugung (beispielsweise durch eine Vielzahl an Photovoltaikanlagen) zu einem Zeitpunkt, an dem der Verbrauch sehr gering ist, kann zu einem Problem bei der Netzlastverteilung werden. Untersuchungen zufolge könnten dezentrale Energieerzeuger in keinem Bundesland die Last decken, wenn weder Windenergie noch Photovoltaik eingespeist werden (Reichl et al 2015). Diese Anlässe stellen i.d.R. zwar besondere Herausforderungen an die Netzsteuerung, waren bisher aber noch beherrschbar oder zumindest lokal begrenzbar. Zu einem Blackout in Folge solcher Ereignisse kommt es meist über Kaskadeneffekte, wenn z. B. durch den Ausfall einer Leitung ohne augenblicklich folgenden Verbraucherabwurf die redundanten Leitungen überlastet werden und ebenfalls ausfallen.

Das (n-1) Kriterium

Grundsätzlich werden Übertragungsnetze mit Hilfe des sogenannten (n-1) Kriteriums[34] geplant, bei dem Redundanzen eine zentrale Rolle spielen. Ausfälle eines Versorgungswegs können so überbrückt werden, ohne dass es dadurch zu Überlastungen in anderen Betriebsmitteln kommt. In der Praxis verfügen Strommasten daher auf beiden Seiten über sechs Leitungen. Drei Leitungen stellen dabei jeweils einen gemeinsamen Stromkreis her. Störungen können so kompensiert werden (Birkmann et al 2010). Bei einem Blackout kommt es zu einem Dominoeffekt, bei dem oft zu hohe Lasten auf einzelne Komponenten einwirken (Missachtung des (n-1)-Kriteriums oder gleichzeitiger Ausfall mehrerer Komponenten), sodass diese

[33] Im Englischen „station blackout“ als Bezeichnung für den Ausfall eines Kraftwerks, das meist nur unter hohem zeitlichen Aufwand wieder angefahren werden kann.

[34] Das (n-1)-Kriterium bezeichnet ein Beurteilungsinstrument für die Redundanz von Systemen. Wenn im Regelbetrieb für eine Funktion n Komponenten verfügbar sind, so muss die Funktion auch mit n-1, also bei Ausfall einer Komponente, weiterhin zu erbringen sein (Strobl 2006, S. 140ff).

schneller ausfallen, als Maßnahmen zur Schadensbegrenzung greifen können. Das führt zu einem großflächigen Stromausfall (entweder geografisch weiträumig, und/oder sehr viele Personen betreffend). Dauert dieser überregionale Ausfall länger (im Bereich mehrerer Stunden bis Tage) spricht man von einem Blackout. Ist die Spannung im Netz vollständig zusammengebrochen, sodass auch Kraftwerke keinen Strom mehr aus dem Netz beziehen können, spricht man auch von einem „Schwarzfall“. In so einer Situation werden sog. schwarzstartfähige Kraftwerke benötigt, die ohne externe Stromversorgung den Betrieb aufnehmen können. Das sind generell Flusskraftwerke, Speicherkraftwerke und dafür ausgerüstete Gasturbinenkraftwerke. Der so gewonnene Strom wird einerseits verwendet, um den 50Hz-Takt im Netz vorzugeben und andererseits, um damit andere, nicht schwarzstartfähige Kraftwerke, wieder anfahren zu können.

Stromausfall
Blackout
Schwarzfall

4.1.1 Kurzübersicht – Stromnetz in Österreich

Das österreichische Übertragungsnetz auf den Spannungsebenen 110, 220 und 380 kV wird von der Austrian Power Grid AG (APG, eine 100 % Tochtergesellschaft der Verbund AG) als Regelzonenführer geregelt. Sie betreut damit eine Gesamtnetzlänge von 6.977 km, auf einer Trassenlänge von 3.400 km, mit ca. 12.000 Masten, 63 Umspann- und Schaltanlagen und einer Transportleistung im Jahr 2014 von 43.957 GWh (APG 2014). Das österreichische Übertragungsnetz ist Teil des europäischen Übertragungsnetzes der Regional Group Continental Europe (RG CE) der Vereinigung der europäischen Übertragungsnetzbetreiber (ENTSO-E). Die APG nimmt eine zunehmend gestalterische Rolle in der Vereinigung der europäischen Übertragungsnetzbetreiber ein. So wurde unter ihrem Vorsitz in den Arbeitsgruppen die wichtigen Network Codes „Operational Security Code“ und „Balancing Code“ entwickelt.

APG als Regelzonenführer

Der Netzausbauplan (NEP) der APG sieht als einen der wichtigen Meilensteine den Schluss des geplanten 380 kV-Rings in Salzburg vor, womit die Netzknoten St. Peter und Tauern mittels 380 kV-Leitung verbunden werden sollen. Bei positivem Abschluss der UVP ist mit einem Baubeginn 2017 zu rechnen. Das würde durch die höhere Übertragungskapazität und die Ringförmigkeit der Verbindung die Ausfallsicherheit stark erhöhen. Weiters müssen die Anbindungen an die nachbarstaatlichen Übertragungsnetze ausgebaut werden, um bspw. den Strom aus erneuerbarer Erzeugung aus Deutschland zu Verbrauchern in Österreich und zu den österreichischen Pumpspeicherkraftwerken leiten zu können (APG 2014, S.19ff).

Netzausbauplan (NEP) und 380 kV-Ring

Durch die geographischen Gegebenheiten in Österreich unterscheidet sich das österreichische Stromnetz in manchen Belangen von dem anderer Länder. Der dominierende Einflussfaktor sind hier natürlich die Alpen, die Netzführung und Engmaschigkeit vorgeben, und selbst einen wenig leitfähigen Untergrund darstellen, durch den ein Spannungsausgleich bei unterschiedlicher Belastung zweier Leitungsenden unwahrscheinlicher ist, als bei feuchtem, leitfähigem Untergrund.

Die Kraftwerke in Österreich sind zu einem vergleichsweise hohen Prozentsatz schwarzstartfähig, da es viele Fluss- und Speicherkraftwerke gibt:[35] insgesamt 93 Anlagen über zehn MW und einer installierten Leistung von knapp 4.500 MW in Laufkraftwerken. Zusätzlich gibt es über 67 Speicherkraftwerke mit einer Leistung über zehn MW und knapp 7.700 MW (Österreichs Energie 2015).

Hohe Versorgungssicherheit in Österreich

Österreich weist eine hohe Versorgungssicherheit aus[36] und es gibt wenig Empirie für größere Stromausfälle mit Blackout-Charakter. Ende der 1970er Jahre ereignete sich ein Fall, bei einem größeren Ausfall in Europa im Jahr 2006 waren einige Länder, darunter auch Österreich betroffen und bis zu 120 Minuten ohne Strom.[37] 2012 konnte u. a. mithilfe Österreichs ein Kollaps des süddeutschen Stromnetzes verhindert werden.[38] Diese Fälle verdeutlichen die hohe Bedeutung von Abhängigkeiten im Stromnetz.

4.1.2 Auswirkungen eines Blackouts

In Österreich wurden u. a. vom Energieinstitut der JKU Untersuchungen zu Blackouts mit technischem Fokus und Versorgungssicherheit durchgeführt, die sehr detailliert mit unterschiedlichen Szenarien auf mögliche Probleme der Lastverteilung im Stromnetz eingehen (vgl. Reichl/Schmidttaler 2011; Reichl et al 2015). Unter anderem wird darin verdeutlicht, dass die Versorgungssicherheit in Österreich stark von den Netzausbaumaßnahmen im europäischen Stromverbundnetz abhängt. Die Netzlast hat eine Auswirkung auf die Aufnahmekapazität. Wenn der Regelbetrieb wenig Pufferkapazität aufweist, können Störungen leichter zu spürbaren Problemen führen. Aus der steigenden Zahl strombetriebener Geräte ergibt sich ein grundsätzlicher Bedarf nach einer besseren Lastverteilung im Stromnetz, um dem gesteigerten Energiekonsum gerecht werden zu können. Kurz gefasst kann eine permanent hohe Netzbelastung das Risiko von Blackouts begünstigen. Für konkrete technische Aspekte und Details sei jedoch auf oben angeführte Studien verwiesen. Mit den gesellschaftlichen Folgen eines Blackouts hat sich eine umfassende Studie des Büros für Technikfolgenabschätzung des Deutschen Bundestages (TAB) eingehend mit den Auswirkungen eines Blackouts beschäftigt (Petermann et al 2011). Im Folgenden wird daher nur eine kurze Zusammenfassung der wichtigen Auswirkungen eines Blackouts auf kritische Bereiche gezeigt.

Hohe Netzlast als Risiko

[35] Gut illustriert auf der online verfügbaren interaktiven Kraftwerkskarte: oesterreichsenergie.at/interaktivekraftwerkskarte.

[36] http://oesterreichsenergie.at/ausfalls-und-stoerstatistik.html

[37] de.wikipedia.org/wiki/Stromausfall_in_Europa_im_November_2006.

[38] www.ksta.de/wirtschaft/zusammenbruch-stromnetz-waere-fast-kollabiert,15187248,16617996.html.

Transport- und Verkehrswesen

Stillstand

Im Transport- und Verkehrswesen sind alle elektrisch betriebenen Elemente von Straße, Schiene, Luft und Wasser betroffen und fallen unmittelbar oder nach wenigen Stunden aus. Betroffen sind vor allem die Infrastrukturen wie Verkehrsleitsysteme, Steuerungssysteme, aber in Folge auch abhängige Transportmittel. Besonders kritisch ist der Schienenverkehr, der abrupt zum Stillstand kommt. In Ballungszentren sind chaotische Zustände des motorisierten Individual- und öffentlichen Personennahverkehrs und zahlreiche Unfälle vor allem in dichtbesiedelten Gebieten wahrscheinlich. Einzig Flughäfen könnten durch Notversorgungen weniger stark betroffen sein. Kritisch ist hier vor allem der Ausfall des Tanknetzes, da es für die Notversorgung etwa von Fahrzeugen und Dieselgeneratoren usw. essentiell ist. Bei Industrieanlagen kann es zu erhöhten Brandrisiken kommen, da Kühlanlagen nicht mehr funktionieren.

Grundversorgung

Beeinträchtigte Ver- und Entsorgung

Die Wasserversorgung wird vielerorts über elektrisch betriebene Pumpen bereitgestellt, die bei einem lang anhaltenden Stromausfall auch nicht mehr zur Verfügung stünden. Das hätte nicht nur Konsequenzen für die Trinkwasserversorgung, sondern könnte auch im Bereich der Hygiene problematisch werden, wenn bspw. Toiletten nicht mehr mit Wasser versorgt werden. Eine Ausnahme stellen natürlich Gebiete dar, die ähnlich wie in Wien, das Trinkwasser aus höheren Regionen beziehen. Jedoch würde nach Einschätzung von Experten der Wasserdruck ohne Pumpen in Wien nicht für höhergelegene Häuser mit mehreren Stockwerken reichen. Darüber hinaus gibt es auch in der Bundeshauptstadt nördlich der Donau Gebiete, die mit Brunnen versorgt werden. Dort fiele die Wasserversorgung komplett aus. Auch die Kläranlagen benötigen Strom, und in vielen Abwassersystemen kommen Hebepumpen zum Einsatz. D. h., dass in weiterer Folge auch der Abtransport des Gebrauchtwassers nicht funktionieren würde. Ein Worst-Case-Szenario wäre in so einem Fall der Ausfall der Kläranlage(n) einer Millionenstadt wie Wien. Ein Einleiten der ungeklärten Abwässer einer großen Stadt in den nahegelegenen Flusslauf wäre ökologisch höchst problematisch. Was die Versorgung mit Essen betrifft, ist zu berücksichtigen, dass die meisten Kochstellen nicht verfügbar wären. Eine Verwendung von Camping-Kochern in geschlossenen Räumen würde das Brandrisiko deutlich erhöhen. Lebensmittelvorräte in städtischen Haushalten sind nach professioneller Einschätzung innerhalb weniger Tage aufgebraucht. Kühlschränke und Tiefkühler würden ebenso wenig funktionieren, wie die Logistik für Lebensmittelhändler, Supermärkte, Tankstellen sowie deren Bezahlsysteme. Durch den Ausfall von Bankomaten wäre auch die Versorgung der Bevölkerung mit Bargeld schwierig. Zudem sind Bezahlvorgänge kaum möglich, da auch elektronische Kassen zur Ein- und Ausgabe von Bargeld nicht mehr nutzbar sind.

Neben einem Zusammenbruch von Logistik und Lagerhaltung im Lebensmittelbereich ist auch damit zu rechnen, dass die Produktion stark eingeschränkt wird. Besonders die hoch automatisierte Produktion in Betrieben würde zum Erliegen kommen. In großen Aufzuchtbetrieben würden die Belüftung und die Fütterungsautomatik ausfallen, sodass nicht nur keine tierischen Lebensmittel mehr hergestellt werden könnten, sondern auch die betroffenen Tiere verenden würden. Das ist zwar besonders unter dem Aspekt einer ethisch vertretbaren Tierhaltung problematisch, kann aber über lange Sicht auch aus hygienischen Gründen zum Problem werden.

Gesundheit

Im Falle eines Blackouts ist die gesamte Gesundheitsversorgung durch Notstrom-versorgte Krankenhäuser abzuwickeln, die ihrerseits jedoch nur einen eingeschränkten Betrieb anbieten können, bei möglicherweise erhöhtem PatientInnenaufkommen. Sollte der Strommangel länger anhalten, kann auch die Logistik im Gesundheitswesen zum Engpass werden. Medikamente werden von Apotheken, so diese aufsperren, nicht mehr bereitgestellt werden können, weil die Lagerkapazitäten nicht vorhanden sind; und in Spitälern wird die derzeit von Experten immer wieder kritisierte tägliche Just-in-Time-Anlieferung von Bedarfsgütern aus dem Ausland nicht mehr klappen, was weitere Restriktionen im (Operations-)Betrieb nach sich zöge.

Just-in-time-Anlieferung im Krisenfall ein Problem

Privathaushalte

Die wenigsten Privathaushalte sind für einen längeren Stromausfall gerüstet. Neben Taschenlampen, Batterien, batteriebetriebenen Radios bedarf es vor allem der ausreichenden Versorgung mit lebensnotwendigen Medikamenten, Trinkwasser und Essen; in der kalten Jahreszeit muss vor allem in der Stadt, wo etwa seltener mit Holz und Kamin geheizt werden kann, auch für ausreichend Wärme gesorgt werden. Die meisten Zentralheizungssysteme werden ausfallen, weil weder die Umlaufpumpen mit Strom versorgt werden können, noch die Steuerungselektronik. In manchen Fällen braucht auch der Zündfunke in Gasbrennern elektrischen Strom. Da die Nahversorgung innerstädtisch im Normalfall sehr gut ist, werden weniger Lebensmittel bevorratet als in ländlichen Regionen, wo es auf Grund des längeren Anfahrtsweges aufwendiger ist, den nächsten Supermarkt zu erreichen. Hier könnten Maßnahmen zur Erhöhung der Resilienz gegen derartige Ausfälle ansetzen, da nach Meinung einschlägiger Experten keine Organisation (Zivilschutz, Rotes Kreuz, Bundesheer o. a.) in der Lage ist, österreichweit alle Menschen über mehrere Tage und Wochen mit Wasser und Nahrungsmitteln zu versorgen, die auf einen längeren Stromausfall nicht vorbereitet sind. In Wohnhäusern mit Aufzugsanlagen ist damit zu rechnen, dass auch Menschen in Aufzügen festsitzen. Das könnte zusätzliche Herausforderungen für die Einsatzkräfte bringen (Wimmer 2015).

Unterschiede zwischen Stadt und Land

Notkommunikation

Gerade in Ausnahmesituationen steigt das Kommunikationsbedürfnis der Menschen. Die laufende Informierung der Bevölkerung ist daher essentiell. Einerseits geht es darum, Informationen zu bekommen (Wer ist aller betroffen? Gibt es Informationen von offizieller Stelle? Wie lange wird der Ausfall dauern? Welche Verkehrsmittel stehen noch zur Verfügung? Kann man irgendwo bei der Beseitigung von Problemen helfen?), andererseits sind soziales Umfeld und sozialer Zusammenhalt wichtig und dementsprechend steigt das Kommunikationsbedürfnis um sicherzugehen, dass es nahe stehenden Personen gut geht und um sich organisieren zu können usw. Das kann dazu führen, dass die Kommunikationsnetze überlastet werden, und verbleibende Ressourcen deutlich schneller aufgebraucht werden als geplant. Betreiber von Mediendiensten, wie Rundfunkanstalten, müssen daher auch in der Lage sein, einen Notbetrieb (bspw. mit reduziertem Personal auf weniger Frequenzen) über einige Tage nach einem Ausfall aufrecht zu halten. Das schließt natürlich auch eine Notstromversorgung aller Sendeanlagen mit ein. Aus Sicht der Betreiber kritischer Infrastrukturen ergibt sich ein weiteres Problem: Wie erreiche ich die MitarbeiterInnen, die ich in so einer Situation brauche? Hier ist Schulung des relevanten Personals und klare Zuständigkeiten im Betrieb (etwa Journaldienste) wesentlich für Vorsorge, um schon im Vorfeld darüber in Kenntnis zu sein, wer sich im Fall eines Stromausfalls (oder einer anderen Krise) wo einzufinden hat.

Massenkommunikation (Radio) zur Information notwendig

Netzbetrieb

Im Falle eines Blackouts ist der Netzbetrieb zusammengebrochen. Je nach Ursache, kann es sein, dass voneinander getrennte Inselnetze entstanden sind, die es gilt wieder miteinander zu verbinden und zu synchronisieren. Oder dass eine große Region ausgefallen ist, das europäische Verbundnetz rundherum aber noch funktioniert. Oder dass schlussendlich ein überwiegender Teil der Synchronzone[39] ausgefallen ist. Am einfachsten lässt sich das Problem beheben, wenn eine Region ausgefallen ist, das Netz rundherum aber noch „gesund“ ist. Dann können die ausgefallenen Bereiche Schritt um Schritt wieder zugeschaltet werden. Ist beispielsweise die Hälfte des europäischen Verbundnetzes spannungslos, dann muss das Netz segmentiert werden. Es werden Inselnetze geschaffen, in denen schwarzstartfähige Kraftwerke hochgefahren werden, dann werden die ersten Verbraucher zugeschaltet. Diesen Prozess wiederholt man Stück um Stück, während die Balance zwischen Produktion und Verbrauch auch in dieser Situation, in der es keine Puffer oder Reserven gibt, gehalten werden muss, bis immer mehr eigenständige Inselnetze laufen. Diese werden in weiterer Folge wieder synchronisiert und zusammengeschaltet. Das

Schrittweiser Wiederaufbau

[39] Das ist ein Teil eines Verbundnetzes, der synchronisiert läuft, d. h. es existiert eine direkte Dreh- oder Wechselstrom-Phasenverbindung zwischen den Teilnetzen einzelner Übertragungsnetzbetreiber (vgl. https://de.scribd.com/doc/295722803/Eps-HS09-Skript-de-01).

Problem an dieser Betriebsart besteht darin, dass sie im Normalbetrieb nie vorkommt. D. h. es wird zwar sehr genau vorbereitet und mit den Kraftwerksbetreibern geübt, aber letztendlich weiß man erst im Ernstfall, ob die Konzepte funktionieren. Über Simulationen wird auch der europäische Netzwiederaufbau geübt. In Österreich hat nicht nur der Übertragungsnetzbetreiber, sondern jeder Verteilnetzbetreiber ein Netzwiederaufbaukonzept, das nach jeder Übung und Simulation justiert und an neue Anforderungen angepasst wird. Diese Konzepte liegen an den relevanten Stellen auf, sodass im Ernstfall jeder weiß, was in welcher Reihenfolge zu tun ist. Bei Ausfall einzelner Steuerungsebenen kann auf die darunter liegende Ebene, bis hin zum Kraftwerk selbst, delegiert werden. Die Kommunikation erfolgt über ein eigenes redundantes Netz, das die regionalen Einheiten miteinander verbindet. Auf Grund der Erzeugerstruktur, mit vielen Flusskraftwerken, die flexibler betrieben werden können als bspw. Gaskraftwerke, und dem großen Engagement der APG auf europäischer Ebene hat Österreich in Bereich des Netzwiederaufbaus, gemeinsam mit der Schweiz, im europäischen Verbund eine Vorreiterrolle übernommen.

Das Zusammenspiel der Notfallpläne und Notversorgung

Die Notfallkommunikation ist im Blackout-Fall essentiell. Nach Reichl et al (2015, S. 399) können mögliche Informations- und Kommunikationswege aus folgenden Wegen bestehen (eigene, vereinfachte Darstellung):

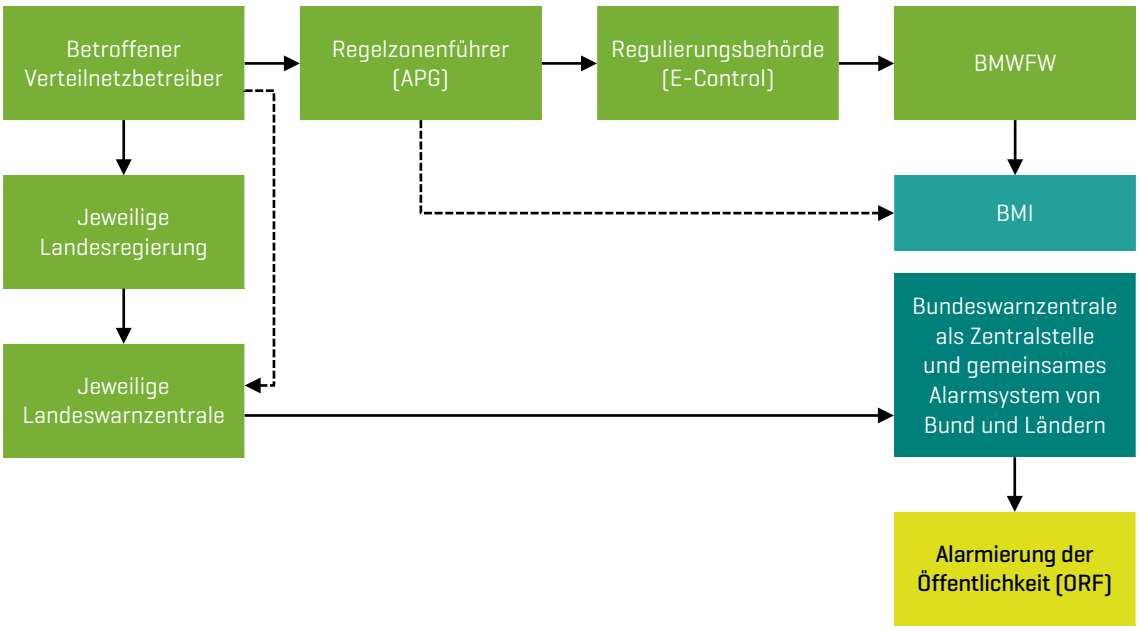

Abbildung 5: Mögliche Informations- und Kommunikationswege im Blackout-Fall

Da die meisten Infrastrukturen heute nicht mehr ohne Stromversorgung funktionieren, und ein Ausfall auch bei der in Österreich grundsätzlich hohen Versorgungssicherheit (Dax 2015) immer wieder passieren kann, haben viele Organisationen für diesen Fall vorgesorgt. Dort, wo Strom unerlässlich ist, gibt es vielfach Notstromversorgungen über Akkus und/oder Generatoren. In anderen Fällen ist zumindest klar, wie die wesentlichen Dienstleistungen auch ohne Strom erbracht werden können. Es ist davon auszugehen, dass die zuständigen Behörden (BMI, Landesverteidigung) über die Verfügbarkeit von Notstromaggregaten und Ressourcen (insbesondere Treibstoff) Bescheid wissen. Wie detailliert hierbei Wissen über die konkrete Notversorgung von einzelnen Einrichtungen vorliegt, konnte allerdings nicht festgestellt werden.

Alle Kritischen Infrastrukturen funktionieren in so einer Situation nur noch eingeschränkt, bspw. wird oft die Beleuchtung und Klimatisierung reduziert. Dort, wo nur Stromspeicher verwendet werden, aber keine Generatoren zur Stromerzeugung vorhanden sind, wird in der Regel versucht, die laufenden Prozesse kurzfristig aufrecht zu erhalten und dann geordnet zu beenden. Dadurch können Schwankungen im Netz und kurze Ausfälle überbrückt werden, bei längeren Ausfällen wird die Infrastruktur in einen Zustand gebracht, der beim Wiederanlaufen nötig bzw. vorhersehbar ist.

Wenn möglich geordnetes Abstellen

Die Wiener Linien können bspw. noch alle U-Bahn-Züge bis zur nächsten Station bewegen, um dort die Fahrgäste aussteigen zu lassen. Dadurch sind die Züge später leicht zugänglich und eine Evakuierung aus Tunnels oder von Brücken wird vermieden.

Mobilfunkanbieter haben eine große Anzahl der Basisstationen mit Akkus ausgerüstet, um Stromausfälle zu überbrücken. Bei einem länger anhaltenden Engpass wird der Dienst weiterhin so lange zur Verfügung stehen, bis nur mehr die Strommenge im Speicher ist, die für das Herunterfahren der Systeme erforderlich ist. Dadurch entsteht, die sog. „Golden Hour", der Zeitraum nach dem Eintreten eines Blackouts, in dem noch viele Menschen erreichbar sind. In der Praxis wird es sich auch auf Grund des zunehmenden Kommunikationsbedürfnisses der KundInnen laut Experten-Einschätzung eher um eine Viertelstunde handeln.

„Golden Hour"

Andere Infrastrukturen wie Krankenhäuser, oder auch große Internet-Knoten, wie der Vienna Internet Exchange (VIX), überbrücken mit schnell schaltenden Notstromversorgungen auf Akku-Basis kurze Ausfälle oder bei längeren Ausfällen die Zeit bis zum Anlaufen der Dieselgeneratoren, die danach für eine kontinuierliche Stromversorgung sorgen sollen. Im Idealfall wird die Funktionstüchtigkeit dieser Komponenten regelmäßig überprüft und der Ablauf im Krisenfall geübt. Meist finden diese Übungen aber nur organisationsintern statt. Das heißt, das Wissen darüber, was passiert, wenn alle Betreiber kritischer Infrastrukturen ihre jeweiligen Notfallpläne in die Tat umsetzen, ist begrenzt. So sind für die Fälle langanhaltender Unterversorgung oft Verträge mit Treibstofflieferanten abgeschlossen worden, die in so einer Situation mit LKWs den Dieselnachschub anliefern sollen. Das funktioniert gut, wenn der Ausfall nur kleinräumig ist. Wäre eine ganze Stadt von dem Blackout betroffen, kann es sein, dass

Notfallübungen zu oft nur organisationsintern

die Treibstoffpumpen an den Tankstellen nicht funktionieren (viele Tankstellen haben weder Notstromaggregate noch eine Einspeisung durch Generatoren vorgesehen), und in weiterer Folge auch nicht ausreichend Kapazitäten zur Belieferung aller Vertragspartner vorhanden sind. Das gleichzeitige Inkraftsetzen aller Katastrophenfallpläne könnte somit schwierig werden, was den unweigerlichen Ausfall als kritisch eingestufter Infrastruktur zur Folge hätte.

„Leuchttürme" als soziale Sammelpunkte

Zusätzlich können andere Herausforderungen auftreten, die so eine Situation vom Normalbetrieb unterscheiden. Beispielsweise könnte es dazu kommen, dass jene Einrichtungen, die bei einem (nächtlichen) Blackout noch Strom haben, und damit wie Leuchttürme weithin sichtbar sind, von großen Teilen der Bevölkerung aufgesucht werden, in der Hoffnung dort Gesellschaft und Informationen zu finden. Dadurch kann es aber zu betrieblichen Einschränkungen kommen, wenn z. B. eine Menschenmenge Zu- oder Abfahrtswege zu Krankenhäusern oder Feuerwachen blockiert. Aus diesem Grund wird in einem Forschungsprojekt in Berlin derzeit untersucht, ob eine sinnvolle Strategie im Falle eines Blackouts in der Einrichtung von „Leuchttürmen" in der Stadt bestehen kann. Das wären bereits bestehende Einrichtungen, wie Bezirksämter, Feuerwachen oder Rettungszentralen, die ausgebaut werden zu zentralen Sammelpunkten, an denen die Menschen mit Informationen und anderen notwendigen Dienstleistungen und Gebrauchsgütern versorgt werden könnten.[40] Eine Studie des Technikfolgenabschätzungsbüros des deutschen Bundestags (TAB) kam 2011 zu dem Schluss, dass bei einem langanhaltenden, großflächigen Blackout der Zusammenbruch des gesellschaftlichen Lebens aus damaliger Sicht kaum vermeidbar wäre, wobei das Problembewusstsein dafür auf allen politischen Entscheidungsebenen, so wie in der Bevölkerung, gering ausgeprägt sei (Petermann 2011, S 238). Das gilt auch für andere Länder und ebenso für Österreich. Allerdings hat sich im Bereich Awareness Building einiges getan. In einigen Ländern (auch in Österreich) befassen sich Behörden verstärkt mit dem Thema Blackout. Insbesondere in der Schweiz wurden hier einige Anstrengungen unternommen. Im November 2014 wurde eine großangelegte Zivilschutzübung durchgeführt, die u. a. eine überregionale Strommangellage simulierte. Dabei stellte sich heraus, dass die Kommunikation mit übergeordneten Stellen bzw. die Meldeketten im Ernstfall ein Problem darstellt, oder wie es von einem Vertreter des teilnehmenden Kantons Waadt festgehalten wurde: „All das, was schon vor der Krise kompliziert ist, ist zum Scheitern verurteilt, sobald das Ereignis eintritt." (Schindler 2014) Das unterstreicht die Wichtigkeit des Krisenmanagements (siehe Abschnitt 5).

[40] Projekt „Kat-Leuchttürme" im Web: kat-leuchtturm.de.

4.2 Informationstechnische Systemabhängigkeiten und Angriffspotenzial

IKT ziehen sich als Querschnittstechnologie mittlerweile ähnlich wie das Stromnetz durch nahezu alle Lebensbereiche. Im Kontext kritischer Infrastruktur lässt sich IKT zum einen selbst als KI-System begreifen. Zum anderen ist IKT die Achillesferse kritischer Infrastrukturen, die sich auch als Schnittstellen-Abhängigkeit begreifen lässt, da sie i.d.R. in Form von unterschiedlichen Schnittstellen an KI-Systeme gekoppelt ist (z. B. über Internet- und/oder – Mobilfunk[41]-Anbindung zur Steuerung, Fernwartung o. dgl.). Je nachdem, ob eine einzelne IKT-Komponente oder mehrere Teile der jeweiligen Infrastruktur (also etwa Unterbrechung der Datenübertragung durch Internet oder Mobilfunk) gestört sind oder ausfallen, kann es hier zu erheblichen Kaskadeneffekten kommen, die etwa zu massiven Beeinträchtigungen des Stromnetzes führen können. Dementsprechend können hier auch gravierende Auswirkungen auf Unternehmen wie private Haushalte entstehen. Eine kritische Komponente innerhalb von KI-Systemen sind insbesondere SCADA-Systeme (Supervisoring Control And Data Acquisition) dar, die schon lange u. a. zur Prozesssteuerung und Automatisierung in technischen Anlagen eingesetzt werden. SCADA-Systeme sind dementsprechend sehr weit verbreitet in kritischen Infrastrukturen wie Energienetzen, der Wasserversorgung, in Verkehrsleitsystemen usw. (vgl. Foster et al 2008).

Steuerungssysteme als kritische Komponenten mit Schwachstellen

Die teilweise veralteten Systeme sind oftmals nicht oder nicht hinreichend auf Vernetzung ausgerichtet bzw. gegen derartige Schwachstellen geschützt. Diese Problematik ist praktisch globaler Natur und daher auch in europäischen Ländern und Österreich gegeben. Experten warnen seit einigen Jahren vor den Schwachstellen dieser Komponenten, da bei der Entwicklung von SCADA-Systemen zum Teil zu wenig Bedacht auf IT-Sicherheit genommen wurde.[42] Ein Beispiel, das weltweit für Aufsehen sorgte ist der Fall Stuxnet[43], ein komplexes Computerschadprogramm (Wurm) der gezielt zur Überwachung und Steuerung von SCADA-Systemen eingesetzt wurde. Hohen Bekanntheitsgrad erlangte Stuxnet 2010, nachdem er auf Computer des Iranischen Atomkraftwerks Buschehr[44] und anderen Industrieanlagen im Iran entdeckt wurde. Sein Ursprung wird in Geheimdienstkreisen vermutet und Gerüchten zufolge soll die Schadsoftware aus der Feder der NSA stammen. Klare Belege gibt es hierfür aber nicht. Stuxnet gilt als Art „first digital weapon“ und damit als Blaupause für die Verwund-

[41] Mobilfunk gewinnt etwa im Bereich Machine-to-Machine (M2M) Kommunikation an Bedeutung, wo teils Prozesse automatisiert werden. Anwendungen reichen hier vom Bereich Industrie 4.0 und Produktionsautomation, Internet der Dinge, bis zu neueren Trends selbstfahrender Autos etc.

[42] derstandard.at/2000020125632/Sicherheitsluecken-Wie-Hacker-ein-Atomkraftwerk-uebernehmen-koennen.

[43] de.wikipedia.org/wiki/Stuxnet.

[44] heise.de/newsticker/meldung/Iran-bestaetigt-Cyber-Angriff-durch-Stuxnet-Update-1096365.html.

barkeit von kritischen Steuerungssystemen.[45] Die Gefahren derartiger Angriffe sind zwar schon seit längerem bekannt, dennoch scheint es nach wie vor erhebliche Sicherheitsmängel zu geben, die diese Angriffe erst ermöglichen. Eine jüngere Studie zeigt teils gravierende IT-Sicherheitsmängel in AKWs auf. Angriffe auf SCADA-Systeme, wie jene von Stuxnet seien demnach auch heute keine Seltenheit und kommen immer wieder vor. Möglich sind solche Angriffe vor allem durch mangelnde Sicherheitskonzepte. Die Studie fand etwa heraus, dass ein französisches AKW sogar direkt über das Internet erreichbar war. Aber auch abseits solcher Extremfälle fehlt es an Organisation und Kommunikation im Umgang mit Sicherheitsproblemen zwischen IT-Sicherheitspersonal und Betriebspersonal. Zudem sei IT-Security oftmals an externe Dienstleister ausgelagert und daher nicht am Standort verfügbar (Baylon/Brunt/Livingstone 2015). Dass hier Gefahren bestehen, zeigt auch ein Fall in Deutschland: erst kürzlich wurde bekannt, dass die Schadsoftware Conficker auf Rechnern des deutschen AKWs Gundremmingen entdeckt wurde. Die Software versuchte, eine Internetverbindung aufzubauen, was aber misslang, da lt. AKW-Betreiber die IT-Systeme nicht mit dem Internet verbunden sind.[46] Auch Conficker ist in Fachkreisen schon lange bekannt und hat seit dem ersten Auftreten 2008 einigen Schaden angerichtet. U. a. waren auch mehrere hundert Rechner der deutschen Bundeswehr mit dem Schädling befallen.[47] Da SCADA-Systeme nicht nur wesentlicher Bestandteil von AKWs sondern auch von anderen kritischen Infrastrukturen sind, ist die Gefahr von derartigen Angriffen auch in anderen Bereichen gegeben. Auch hierfür gibt es ein Beispiel: im Dezember 2015 wurde in der Ukraine in großflächiger Stromausfall durch Einsatz von Schadsoftware (vermutet wird der Schädling „Blackenergy“) herbeigeführt. Dabei wurden drei lokale Strombetreiber angegriffen. Von diesem Angriff war die Stromversorgung von rund 225.000 Haushalten für mehrere Stunden betroffen.[48] Angriffsbedingte Ausfälle gibt es auch in anderen Ländern, wenngleich nicht in diesem Ausmaß. So kam es etwa im November 2016 in zwei Wohnanlagen im finnischen Ort Lappeenranta zu einem Ausfall der Heizungssteuerung aufgrund einer DDOS-Attacke.[49] Entwicklungen im Bereich Internet-der-Dinge (IoT), Smart Home etc. können die Möglichkeit von DDOS-Angriffen begünstigen. Etwa, in dem internetfähige Haushaltsgeräte zum Aufbau eines Angriffsnetzes missbraucht werden.[50] Auch das US-Energieministerium verzeichnete kürzlich eine Zunahme an Cyber-Attacken auf Energienetze wie

---

45 wired.com/2014/11/countdown-to-zero-day-stuxnet/.

46 golem.de/news/it-sicherheit-schadsoftware-auf-rechnern-im-akw-gundremmingen-entdeckt-1604-120551.html.

47 de.wikipedia.org/wiki/Conficker.

48 golem.de/news/us-untersuchung-hacker-verursachten-tatsaechlich-stromausfall-in-ukraine-1602-119432.html.

49 heise.de/newsticker/meldung/Finnland-DDoS-Attacke-auf-Heizungssteuerung-3459730.html.

50 derstandard.at/2000046354911/Internet-Blackout-System-das-Atomschlaege-ueberlebt-ist-anfaellig-fuer-Toaster.

Strom- und Gasnetzbetreiber in den USA.[51] Auch das Internet der Dinge (IoT) bzw. vernetzte Geräte des Alltags können zur Gefahr werden. SicherheitsforscherInnen demonstrierten anhand einer vernetzten Glühbirne, dass die geringe Sicherheit des für IoT relevante ZigBee-Protokolls enormes Schadenspotenzial bietet.[52] Ein weiteres, neueres Phänomen ist sogenannte „Ransomware" (auch bekannt als Verschlüsselungstrojaner). Das ist Schadsoftware, die versucht, Daten oder Computersysteme zu kapern (z. B. durch versteckte Verschlüsselung), um Geld für die Freigabe zu erpressen. Zu einem solchen Fall kam es etwa 2016 in Krankenhäusern im deutschen Nordrhein-Westfalen, wo per E-Mail eingeschleuste Ransomware zu erheblichen Problemen führte. Eine Analyse des Falles hat zwar ergeben, dass es sich um keinen gezielten, sondern eher einen zufälligen Angriff handelte.[53] Der Störfall war dennoch kritisch, denn das gesamte IT-Netzwerk eines Krankenhauses musste geplant abgeschaltet werden, was zu erheblichen Beeinträchtigungen im Krankenhausbetrieb führte (u. a. verschobene Operationstermine).[54] Der Fall verdeutlicht zum einen, dass Schadsoftware komplexe Risiken mit sich bringen kann. Zum anderen wird deutlich, dass klassische Angriffe (wie per E-Mail) nach wie vor meist sehr einfach durchführbar sind, wenn grundlegende Sicherheitskonzepte fehlen oder mangelhaft sind.

4.2.1 Hyperkonnektivität und wechselseitige Abhängigkeiten

Das Internet als globales Informations- und Kommunikationsmedium durchdringt mittlerweile erhebliche Teile des alltäglichen Lebens und ist zu einer Art Zentrale für Informationsversorgung geworden. Internet-Ausfälle sind dementsprechend kritisch und Ausfälle einzelner Internetserviceprovider kommen immer wieder vor.[55] Allerdings bringt die Beschaffenheit des Netzes, das von Redundanz geprägt ist, eine höhere Bewältigungskapazität mit sich. Totalausfälle etwa ganzer Regionen sind dementsprechend weniger leicht möglich. Ähnliches gilt für Mobilfunknetze, wenngleich es auch hier zu größeren Störungen kommen kann[56]. Ein wichtiger Faktor bei IKT ist die Substituierbarkeit durch alternative Medien wie etwa Telefon oder Mobilfunk. Kritisch können IKT-Ausfälle insbesondere dann werden, wenn durch die Abhängigkeit eine Kaskade ausgelöst wird, etwa daran gekoppelte Systeme wie etwa das Stromnetz oder Teile davon in Folge ebenfalls

---

51 heise.de/newsticker/meldung/US-Energieministerium-Cyberangriffe-auf-Energieversorger-nehmen-zu-3590909.html.

52 heise.de/newsticker/meldung/Licht-an-Licht-aus-ZigBee-Wurm-befaellt-smarte-Gluehbirnen-3459004.html.

53 presseportal.de/blaulicht/pm/58451/3282474.

54 zdnet.de/88259799/computerviren-legen-systeme-mehrerer-kliniken-in-nrw-lahm/.

55 deutsche-wirtschafts-nachrichten.de/2013/08/13/massive-internet-stoerung-bei-der-deutschen-telekom/.

56 heise.de/newsticker/meldung/Grossstoerung-im-Telekom-Mobilfunknetz-1874244.html.

Smart Meter als zusätzliches Risiko

gestört werden. Und vice versa, ein Strom-Blackout hätte auch weitgehende IKT Ausfälle zur Folge. Ein Beispiel für die erhöhte Vulnerabilität durch eine IKT-Abhängigkeit im Stromnetz ist die Einführung von Smart Metern, die eine stärkere Verzahnung von IT und Stromnetz mit sich bringt.[57] Hierbei spiegelt sich die Ambivalenz der Vernetzung deutlich wider: Ein wesentlicher Grund für Smart Metering bzw. Smart Grids ist eine Verbesserung des Lastenmanagements, etwa um Stromspitzen besser im Netz bewältigen zu können. Allerdings erhöht sich dadurch auch die Komplexität des kritischen Infrastruktursystems Strom und seine Verwundbarkeit gegenüber Störungen unterschiedlicher Art. Wo einstmals nur eine einfache Verbindung zwischen Stromzähler und Netz vorhanden war, kommt nun eine IT-Anbindung hinzu. Hier entstehen neue Angriffsflächen, da das Stromnetz dann auch über IKT-Systeme angreifbar ist. Störungen können das Resultat gezielter Angriffe (z. B. Denial of Service Attacken) sein, aber auch durch Softwarefehler entstehen. Auch das öffentliche Verkehrsnetz ist zunehmend vernetzt und mittels IKT-Steuerungssystemen automatisiert. Steuerungs- und Leitsysteme für U-Bahn und Eisenbahn werden auch über IT gesteuert und fahren teils seit Jahren quasi selbständig. Auch in diesem Bereich gibt es Beispiele[58] für Angriffe und ausgenützte Sicherheitsschwachstellen. Der Sicherheitsspezialist Sophos entwickelte eine Test-Simulation namens „HoneyTrain“ zur besseren Analyse von kritischen Sicherheitsaspekten eines Zugsteuerungssystems.[59]

Steigende wechselseitige Abhängigkeit bei zunehmender Vernetzung

Die Grund-Problematik der wechselseitig steigenden Abhängigkeit kann sich auch in anderen Bereichen weiter verschärfen, wenn der Trend zur gesellschaftlichen Hyperkonnektivität, Systemvernetzung und IKT-basierter Automatisierung (wie Machine-2-Machine Kommunikation, Industrie 4.0) weiter an Fahrt gewinnt. Mit der Fortführung des Trends in Richtung vernetzter Systeme steigt auch Verbreitungsgrad von autonomen Systemen wie etwa autonomen Fluggeräten (Drohnen) oder autonomen Fahrzeugen. Deren Einsatz kann einerseits neues Gefahrenpotenzial für kritische Infrastrukturen mit sich bringen, wie etwa das Bespiel von bislang ungeklärten Sichtungen von Drohnen über AKWs zeigt.[60] Andererseits bringen diese quasi-autonomen Systeme durch ihre hohe Komplexität und Automatisierungstendenzen einen erhöhten Bedarf nach wirksamen Sicherheitsmaßnahmen mit sich. Fehler, Störungen oder gezielte Angriffe können hier zu erheblichen Problemen führen. Kürzlich wurde etwa von Sicherheitsforschern demonstriert, wie ein Auto gehackt und ferngesteuert werden kann. Möglich ist das erst durch die Vielzahl elektronischer Komponenten, die vernetzt und wie in diesem Fall häufig schlecht oder gänzlich ungeschützt

---

57 Möchel, E. (2011): Angriffsvektor Stromzählernetz, fm4.orf.at/stories/1685996/.

58 Naone E. (2008): Gehackte U-Bahn, in Technology Review heise.de/tr/artikel/Gehackte-U-Bahn-275506.html.

59 sophos-events.com/honeytrain/aufbau.cfm; golem.de/news/sophos-honeytrain-soll-hacker-in-die-falle-locken-1503-112992.html.

60 spiegel.de/wissenschaft/technik/drohnen-ueber-akw-frankreich-raetselt-ueber-terror-gefahr-a-1005559.html.

per Internet erreichbar sind.[61] Diese Beispiele verdeutlichen, welche Auswirkungen fehlendes Bewusstsein und Kenntnisse der IT-Sicherheit haben können, insbesondere, wenn Systeme mit IT ausgestattet werden, ohne zuvor ein sinnvolles und wirksames Sicherheitskonzept zu erstellen. Experten fordern daher eine strikte Trennung zwischen den Komponenten insbesondere Entkopplung von sensiblen Systemen wie der Fahrzeugsteuerung. Medienberichten zufolge ist unklar, inwieweit Automobilhersteller die Entkopplung der Systeme überhaupt mit Sicherheitstests überprüfen.[62] Hierbei besteht jedenfalls Nachholbedarf. Aber potenzielle Gefahren gehen nicht nur von möglichen Angriffen aus. Auch das Eintreten unerwarteter Phänomene kann Störungen verursachen. Dass kleine Ereignisse große Wirkung haben können zeigt etwa der Ausfall des Autopiloten eines teilautonomen Fahrzeugs: Ursache des Ausfalls war eine große Motte, die den Radar-Sensor des Fahrzeugs verdeckte.[63] Auch dieses Beispiel verdeutlicht, wie wichtig es ist, System-Schnittstellen (wie diesen Sensor) als besonders schutzwürdige Komponenten zu begreifen und dementsprechend bei Schutzkonzepten zu berücksichtigen.

Aufgrund dieser Entwicklungen gewinnt der Bereich IT-Sicherheit bzw. „Cyber-Security“ noch weiter an Bedeutung, bei der Sicherheit als fortlaufender Prozess betrachtet wird. Um derartige Gefahren in kritischen Infrastrukturen zu entschärfen, ist eine striktere Umsetzung von Sicherheitsmaßnahmen hier dringend empfohlen. Brauchbare Ansätze finden sich in bestehenden Standards und Empfehlungen wie sie etwa im Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ des deutschen Bundesverbands der Energiewirtschaft (BDEW 2015) oder dem Security-Kompendium für industrielle Steuerungssysteme des Bundesamts für Sicherheit in der Informationstechnik (BSI 2013) beschrieben sind. Hier gibt es eine breite Palette an Anforderungen wie etwa erhöhten Bedarf nach sicherer Daten-Verschlüsselung bis zur Systementkopplung etc. Bewusstsein und Know-How zur Umsetzung solcher Maßnahmen scheint bislang nur in einzelnen Fachkreisen gegeben und insgesamt eher gering ausgeprägt zu sein.

Entkopplung von Systemen notwendig

61 heise.de/newsticker/meldung/Hacker-steuern-Jeep-Cherokee-fern-2756331.html.

62 heise.de/newsticker/meldung/Experte-fordert-besseren-Schutz-fuer-sensible-Systeme-im-Auto-2769327.html.

63 futurezone.at/digital-life/motte-legt-teslas-autopiloten-lahm/201.565.169.

4.2.2 Satellitenkommunikation als vernachlässigte Abhängigkeit

GPS unterschätzt

Ein Subsystem von IKT, das vielfältig auch in kritischen Infrastrukturen zum Einsatz kommt ist das Satellitenbasierte Global Positioning System (GPS).[64] GPS ist vor allem als Navigationssystem bekannt und weit verbreitet. Tatsächlich ist das Anwendungsspektrum aber wesentlicher breiter[65] und reicht von Navigation im Alltag, verschiedenen Verkehrssystemen (Straßenverkehr, Bahn, Schiff, Flugverkehr) bis zur Zeitsynchronisierung im Finanzwesen, bei IT-Servern und auch Stromnetzen (RAE 2011). Die potenziellen Abhängigkeiten sind hier daher enorm und deren Auswirkungen hängen von der Redundanz und Substituierbarkeit ab. Gibt es keine Alternativen und kommt es zu einem größeren Störfall, können KI-Systeme erheblich gestört werden.

Zeitsynchronisation spielt eine bedeutende Rolle für moderne technische Netzwerke. Dabei kommen häufig GPS-Module zum Einsatz, die GPS-Signale empfangen um die als Zeitgeber fungieren.[66] Diese ermöglichen relativ kostengünstige und präzise Zeitangaben. So benutzen etwa Umspannwerke im Stromnetz teilweise GPS-Signale zur Zeitsynchronisation[67] Aufgrund der n-1 Sicherheit wird zwar i.d.R. gerade im Stromnetz besonders auf Redundanzen geachtet, allerdings ist unklar, inwieweit das grundsätzlich bei KI-Bereichen der Fall ist. Ohne die Verfügbarkeit alternativer Systeme (etwa funkbasierte Synchronisierungssysteme oder lokaler Zeitgeber) kann es bei GPS Ausfall zu erheblichen Problemen kommen.

Zeitsynchronisation im Finanzwesen

Ähnliche Anwendungen finden sich auch im Finanzwesen – der moderne Börsenhandel und das sogenannte High Frequency Trading (HFT) wären ohne präzise Zeitmessungen und laufende Synchronisation nicht möglich. (vgl. Korreng 2011, O'Hara 2011). Dass Zeitsynchronisation ein kritischer Aspekt im modernen Finanzwesen ist, verdeutlicht u. a. das Ausgleichen einer Schaltsekunde am 30.6.2015, bei der Börsen wie die Wall Street frühzeitig geschlossen wurden, um für eine fehlerfreie Umstellung zu sorgen. Fehler bei der Zeitsynchronisation in IT-Systemen können hier mitunter auch zu Ausfällen führen.[68]

Grundsätzlich bestehen verschiedene Möglichkeiten zur Zeitsynchronisierung. Allerdings wird meist eine externe Quelle, die als Zeitgeber fungiert benötigt. Ein GPS-Empfänger ist dabei nur eine Möglichkeit, daneben gibt es auch noch die Möglichkeit per Funk[69] (vgl. RAE 2011). Aufgrund des

---

64 Wurde ab 2000 immer mehr zum Massenprodukt, derstandard.at/2000019222805/20-Jahre-GPS-Wie-das-Navi-zum-Massenprodukt-wurde.

65 gps.gov; gps.gov/applications/timing/.

66 timetoolsglobal.com/information/gps-ntp-server/; en.wikipedia.org/wiki/Clock_synchronization.

67 meinberg.de/german/info/time-synchronization-electrical-systems.htm.

68 handelszeitung.ch/invest/boersen-weltweit-fuerchten-sich-vor-dieser-nacht-805717.

69 Z.B. durch Zeitzeichensender wie DCF77 de.wikipedia.org/wiki/DCF77.

hohen Popularitätsgrades ist GPS aber eine relativ kostengünstige Variante für genaue Zeitangaben, die in vielen technischen Komponenten Verwendung findet. Aus Gründen der Kostenreduktion ist davon auszugehen, dass es Bereiche gibt, wo auf nur ein System gesetzt wird und keine Redundanzen existieren.[70] Dadurch ergibt sich eine erhöhte Abhängigkeit und damit auch ein erhöhtes Störungsrisiko. Zudem existieren eigene Störsender (GPS Jammer), die Schwachstellen von GPS[71] ausnützen können, um GPS-Signale zu stören (vgl. RAE 2011). Um diesem Abhängigkeitsrisiko entgegenzuwirken empfiehlt sich das Vorsehen von Redundanzen, um den Ausfall eines Zeitgebers ggfs. Abfedern zu können. Das ist vor allem bei besonders kritischen Bereichen von Bedeutung, insbesondere bei Systemen zur Krisenkommunikation. Auch das TETRA System (Terrestrial European Trunked Radio Access) das zur Notfallkommunikation benutzt wird, ist abhängig von satellitenbasierter Navigation (Cannon et al 2013). Dass es auch bei Satellitensystemen zu unvorhersehbaren Ausfällen kommen kann, zeigt u. a. der jüngste Vorfall des europäischen Satellitennavigationssystems Galileo, bei dem mehrere Atomuhren aus bislang ungeklärter Ursache ausfielen.[72] Satellitensysteme sind zwar i.d.R. mit mehrfachen Redundanzen abgesichert, allerdings waren bei diesem Vorfall auch einige Ersatzsysteme vom Ausfall betroffen.

Handlungsbedarf: systematische Schwachstellen-Analyse kritischer Infrastruktur-Komponenten

Satellitensysteme sind ein Beispiel für eine verdeckte Systemabhängigkeit, deren Beeinträchtigungen mitunter zu Ausfällen in ganz anderen Bereichen führen können. Da gerade digitale Systeme hochgradig und zunehmend vernetzt sind, ist mit einer Verschärfung dieser Problematik zu rechnen. Es gibt daher Handlungsbedarf nach systematischer Schwachstellen-Analyse kritischer Infrastruktur-Komponenten. Dazu bedarf es einer Identifikation dieser Komponenten in den jeweiligen Bereichen um etwaige Abhängigkeiten im Detail erkennen und dementsprechend vor Ausfall schützen zu können. Diese Maßnahmen sollten Bestandteil des staatlichen Krisenmanagements sein (siehe Abschnitte 5 und 6).

Besondere Beachtung von Satellitensystemen notwendig

Vor dem Hintergrund der in Abschnitt 3 erläuterten Risiken von EMPs und geomagnetischen Strömen kann die Abhängigkeit zu Satellitensystemen als kritisch angesehen werden. Aufgrund der Vielfalt unterschiedlicher Satellitensysteme und Bauweisen gibt es erhebliche Unsicherheiten bezüglich des Verhaltens dieser Systeme durch elektromagnetische Feldstörungen. Ein starker Solarsturm könnte etwa zum Ausfall von satellitenbasierten Navigationssystemen von einem bis zu drei Tagen führen (Cannon et al 2013).[73] Bezüglich dieser Risiken ist die Robustheit von Satellitensys-

[70] In welchen Bereichen dies konkret der Fall ist, ist schwer feststellbar, da oftmals wenig Details zu technischen Komponenten öffentlich zugänglich sind. Eine Anfrage bei der Wiener Börse blieb beispielsweise unbeantwortet. Über dieses Problem scheint gegenwärtig wenig Bewusstsein vorhanden zu sein.

[71] spiegel.de/netzwelt/gadgets/schwachpunkte-des-gps-systems-wenn-das-navi-nicht-weiter-weiss-a-750998.html.

[72] golem.de/news/satellitennavigation-galileo-gehen-die-uhren-aus-1701-125650.html.

[73] ef-magazin.de/2011/03/29/2936-globalisierung-dringende-warnung-vor-ausfall-des-gps.

temen und ggfs. Alternativen ein wichtiges Thema (vgl. RAE 2011). Satelliten sind bis zu einem gewissen Grad abschirmbar und i.d.R. ähnlich wie militärisches Gerät gehärtet. Neuere Satelliten könnten auch so gestaltet werden, dass sie im Falle einer Änderung der Frequenz durch Umschalten/Anpassen auf die andere Frequenz wieder senden können. Dazu müssten natürlich auch die Empfangsgeräte dementsprechend in der Lage sein, das Signal zu verarbeiten. Ein Kernproblem von Systemabhängigkeiten und der daraus resultierenden Vulnerabilität sind fehlende Sicherheitspuffer bzw. mangelnde Redundanz. Hierbei spielen ökonomische Rahmenbedingungen teilweise eine Rolle. Einst staatlich betriebene Infrastruktur ist durch Marktliberalisierung und Privatisierungen verstärkt auch Marktmechanismen wie Wettbewerbs- und Preisdruck ausgesetzt, wodurch Sicherheitsvorkehrungen wie Redundanzen und andere Sicherheitspuffer teilweise aus Kostengründen rückläufig sind.

5 Sicherheit und Krisenmanagement in Österreich

5.1 Überblick – Strategische Programme zu Sicherheit und kritischer Infrastruktur

Als gesamtstaatliche Aufgabe ist der Schutz kritischer Infrastrukturen strategisch eng mit dem Bereich der nationalen Sicherheit und dem staatlichen Krisen- und Katastrophenschutzmanagement (SKKM) verbunden. Dieser Abschnitt zeigt einen kurzen Überblick über die verschiedenen miteinander verzahnten Strategien. Im Anschluss wird näher auf Österreichs Programm zum Schutz kritischer Infrastrukturen (APCIP[74]) eingegangen. Eine Einschätzung und Handlungsempfehlungen folgen in Abschnitt 6.

Österreichische Sicherheitsstrategie (ÖSS)

Ein zentraler Baustein für die nationale Sicherheit ist die Österreichische Sicherheitsstrategie (ÖSS), die als Rahmenwerk verstanden werden kann. Dementsprechend umfassend sind die Zielsetzungen (hier seien nur einige genannt): u. a. umfassender Schutz der Bevölkerung, Gewährleistung der territorialen Integrität und der Selbstbestimmung, Schutz der Verfassung und der Grundrechte, Stärkung des Gemeinwohls, Aufrechterhaltung des sozialen Friedens, Sicherstellung der Verfügbarkeit lebensnotwendiger Ressourcen, Umweltschutz, Kampf gegen Terrorismus und organisierte Kriminalität, Cyber-Angriffe und -Kriminalität, Eindämmung illegaler Migration und Bekämpfung der Schlepperei, Krisenfrüherkennung, -bewältigung und -nachsorge, bis zur Förderung des Sicherheitsbewusstseins in der Bevölkerung, und dem Schutz kritischer Infrastrukturen (BKA 2013a). Die ÖSS ist stark auf die Schaffung eines holistischen Sicherheitsansatzes ausgerichtet, wobei es teilweise zu Überschneidungen zwischen inneren, externen sowie zivilen und militärischen Sicherheitsbereichen kommt. Aufgrund der Vielschichtigkeit der Sicherheitsaufgaben ist das zwar teilweise nachvollziehbar, allerdings kann die verstärkte Integration militärischer Sicherheit in zivile Bereiche demokratiepolitisch durchaus problematisch gesehen werden. Dieser Umstand wurde u. a. vom Österreichischen Studienzentrum für Frieden und Konfliktlösung (ÖSFK) kritisiert (ÖSFK 2011).

SKKM 2020 Strategie

Wie aus der ÖSS hervorgeht, umfasst SKKM in Österreich Krisenfrüherkennung, -bewältigung und -nachsorge, also alle Prozesse und Maßnahmen, die vor, während und nach einer Krise/Katastrophe notwendig sind. Das umfasst grundsätzlich auch Maßnahmen zur Prävention, Erhöhung der Resilienz, Bewältigung einer Krisensituation bis hin zum Wiederherstellen des Normalzustands/Regelbetriebs und der folgenden Nachsorge. Zu letzterer ist auch die kontinuierliche Evaluierung der verschiedenen Prozesse zu rechnen. Fundament für die strategische Ausrichtung und Weiterentwicklung des SKKM ist die SKKM 2020 Strategie, deren Grundprinzipien umfassen u. a.: primäre Selbsthilfe in lokalen Strukturen unter subsidiärer Intervention höherer Verwaltungsebenen (in Ländern und Gemeinden; der

[74] Austrian Programme for Critical Infrastructure Protection.

Bund ist nur in spezifischen, überregionalen Fällen zuständig), die Einbeziehung auf ehrenamtlicher Mitarbeit basierender Organisationen, einfacher Zugang der Behörden zu militärischen Assistenzeinsätzen, grenzüberschreitende Kooperation, Gewährleistung der Kooperation und Koordination der zuständigen Stellen aller Gebietskörperschaften und Einsatzkräfte etc. Maßgebliche Ziele sind u. a. Prävention und Risikooptimierung, Früherkennung und Frühwarnung vor Katastrophen und deren Schadenspotential, Sicherstellung eines hohen Niveaus der Einsatzvorbereitung, rasche und effiziente Reaktion auf Katastrophen zur Schadensminimierung für die Allgemeinheit auf nationaler und internationaler Ebene, rascher Übergang zur Normalsituation nach Katastrophen. Die SKKM-Strategie setzt auch verstärkt auf technische Innovationen zur Steigerung der Effizienz von Maßnahmen und des Informationsflusses zwischen strategischen EntscheidungsträgerInnen, sowie der anlassfallbezogenen Kommunikation mit der Bevölkerung. Hierbei ist auch eine stärkere Einbindung von Forschung und Entwicklung angedacht (BMI 2009).

Österreichische Strategie für Cyber-Sicherheit [ÖSCS]

Durch die zunehmende Bedeutung des Cyberraums wurde (wie in der ÖSS vorgesehen) 2013 eine eigene Österreichische Strategie für Cyber-Sicherheit (ÖSCS) geschaffen. Die Umsetzung dieser Strategie ist derzeit im Fluss. D. h. es gibt eine Reihe von Akteuren, die sich mit der Thematik befassen und ihrerseits Maßnahmen setzen (siehe nächster Abschnitt). Die ÖSCS deckt die sicherheitsrelevanten Aspekte der IKT-Strategie des Bundes (IKTS) ab, die IKT vor allem als zentrales Mittel zur Stärkung des wirtschafts- und gesellschaftlichen Wohlstands sieht und E-Government und E-Commerce weiter voranbringen will. Die Koordination obliegt hier primär der Plattform Digitales Österreich (PDÖ)[75]. Die ÖSCS sieht die Offenheit und Freiheit des Internet, den Schutz personenbezogener Daten und die Unversehrtheit miteinander verbundener Netzwerke als Fundament für globalen Wohlstand, Sicherheit und Menschenrechte. Cybersicherheit wird als gesellschaftliche Querschnittsmaterie erachtet, mit dem Ziel die Sicherheit und Resilienz österreichischer Infrastrukturen und Leistungen im Cyberraum zu stärken, sowie Bewusstsein und Vertrauen zu schaffen. Ein Schwerpunkt liegt auf IKT-Schutz und der Einrichtung eines Cyber-Krisenmanagements unter Einbindung von Cyber Emergency Response Teams (CERTs). Die Maßnahmen der ÖSCS sind als Ergänzung und Vertiefung zum APCIP bezüglich Cybersicherheit zu verstehen (BKA 2013b). Den zentralen Baustein für den Schutz kritischer Infrastrukturen bildet schließlich das APCIP, auf das ÖSS und ÖSCS Bezug nehmen (das im Abschnitt 5.3 näher erläutert wird). Im Folgenden wird das Zusammenspiel einiger zentrale Akteure mit Bezug zu den genannten Strategien, insbesondere SKKM und APCIP, kurz skizziert.

75 digitales.oesterreich.gv.at/site/7584/default.aspx.

5.2 Übersicht zentraler Akteure in Österreich

Durch die vielfältige Verankerung kritischer Infrastrukturen in der Gesellschaft sind naturgemäß eine Reihe unterschiedlicher Akteure für die Thematik relevant. Die Vielfalt der Akteure und Strategien verdeutlicht einerseits die Komplexität der Problematik andererseits aber auch die teils unklaren Zuständigkeiten. Die folgende Grafik zeigt eine kompakte Übersicht der wichtigsten Akteursgruppen (ohne Anspruch auf Vollständigkeit) mit Fokus auf SKKM und APCIP in Österreich. Für das bessere Verständnis der in 5.1 angeführten Strategien sowie der Rolle von IKT und Cyber-Sicherheit wurden diese Teile hier mitmodelliert:

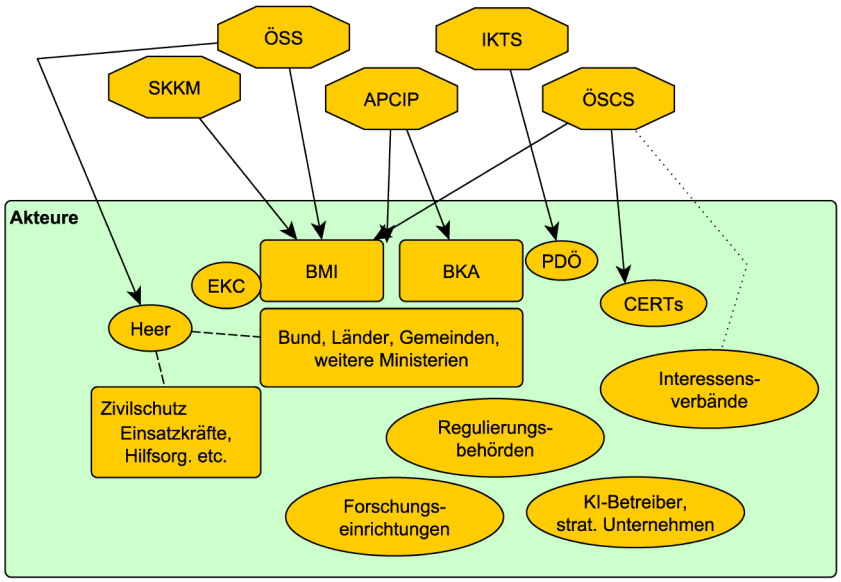

Abbildung 6: Übersicht zentraler Akteure

Nachdem die Daseinsvorsorge eine genuin staatliche Aufgabe ist, nehmen staatliche Institutionen einen zentralen Stellenwert ein. Das staatliche Krisen- und Katastrophenschutzmanagement (SKKM) ist in Österreich eine verteilte Aufgabe von Bund, Ländern und Gemeinden. Die Koordination obliegt in erster Linie dem Bundesministerium für Inneres (BMI). Seit 2004 ist das dort angesiedelte Einsatz- und Krisenkoordinations-Center (EKC) die zentrale Informations-, Kommunikations- und Koordinationsplattform in Österreich für Katastrophen- und Krisenmanagement. Das EKC betreibt auch die Bundeswarnzentrale, die als Informationsdrehscheibe des Bundes zur Koordination von Hilfsmaßnahmen bei Großschadensereignissen fungiert und permanent besetzt ist. Im BMI werden koordinative Aufgaben für KKM sowie für die internationale Katastrophenhilfe durchgeführt. Nach dem Subsidiaritätsprinzip sind vor allem die Bundesländer und Gemeinden in hoher Eigenverantwortung für konkrete Maßnahmen zuständig, da sie i.d.R. die geringste Distanz zu Krisenherden und Katastrophenschauplätzen haben. Hierbei nimmt auch die Zivilgesellschaft und ehrenamtliche

Das Center für Krisenkoordination (EKC) als zentrale Informations-, Kommunikations- und Koordinationsplattform in Österreich für Katastrophen- und Krisenmanagement

Tätigkeit (vor allem bei Rettungskräften wie Rotem Kreuz und Feuerwehr[76]) eine zentrale Funktion ein. Im Bedarfsfall kommt auch das Bundesheer zum Einsatz, das neben der Landesverteidigung auf behördliche Anforderung auch mit umfassenden Aufgaben für (Selbst-)Schutz und Hilfe der Bevölkerung betraut werden kann. Für die Einbeziehung und Bewusstseinsbildung der Bevölkerung in Krisen- und Katastrophenschutz (z. B. durch Informationsmaterial, Veranstaltungen, Schulungen etc.) sind die in den Ländern eingerichteten Zivilschutzverbände zuständig (vgl. SKKM 2009, Jachs 2014). Für die Führungsaufgaben im Katastrophenfall wurde 2007 eine Richtlinie geschaffen, um die Einsatzführung stärker zu vereinheitlichen (BMI 2007).

Plattform Digitales Österreich [PDÖ]

Für die Koordination des staatlichen Gesamtprozesses im Bereich Schutz kritischer Infrastrukturen (CIP – Critical Infrastructure Protection) sind vor allem das Bundeskanzleramt (BKA) und das Bundesministerium für Inneres (BMI) verantwortlich. In den Kompetenzbereich des BKA fällt unabhängig vom APCIP auch die IKT-Strategie des Bundes (IKTS). Für die Koordination und Strategieentwicklung ist die Plattform Digitales Österreich (PDÖ) zuständig. Die Cyber-Sicherheitsstrategie ist eng mit der IKTS verbunden. Im Rahmen des APCIP legen BMI und BKA gemeinsam die Liste kritischer Infrastrukturen in Österreich fest (siehe Abschnitt 5.3). und sind in Form von Public Private Partnerships in Kontakt mit Betreibern strategischer Unternehmen und Organisationen. Die einzelnen Ministerien (BMLVS, BMWFW, BMVIT, BMF, BMLFUW, BMG) sowie die Bundesländer sind in Form eines Beirats in das APCIP eingebunden, der sich thematisch einbringt und bei Bedarf eigene Arbeitsgruppen einrichten kann. Neben nationalen Kooperationen und enger Zusammenarbeit mit der EU-Kommission sieht das APCIP auch Partnerschaften mit EU-Mitgliedstaaten wie Deutschland und Schweiz (im Rahmen der D-A-CH Kooperation) sowie Mitgliedsstaaten des Forum Salzburg zur Zusammenarbeit im Feld der inneren Sicherheit[77] vor. Für die Maßnahmen zum KI-Schutz sind primär die KI-Betreiber zuständig. Die Mitarbeit am APCIP erfolgt in Form freiwilliger Kooperationen. Für die Aufgaben und Befugnisse von Sicherheitsbehörden zum KI-Schutz soll ein gesetzlicher Rahmen geschaffen werden (vgl. BKA 2015). Das APCIP setzt stark auf die Kooperation und Eigenverantwortung von KI-Betreibern in allen Sektoren. Als Beispiel angeführt sei hier nur die Austrian Power Grid AG (APG)[78], die das Übertragungsnetz in Österreich betreibt, das aus dem Hochspannungsnetz (380 kV, 220 kV und 110 kV) und mehreren Schalt- und Umspannwerken (63) besteht. Insofern repräsentiert sie eine wichtige Funktion in der kritischen Infrastruktur Stromnetz.

Nationale und internationale Zusammenarbeit und Vernetzung

[76] Hier engagieren sich bspw. weit über 300.000 Freiwillige (vgl. Jachs 2014).

[77] Teilnehmende Staaten des Forum Salzburg sind neben Österreich: Bulgarien, Kroatien, Polen, Rumänien, Slowakei, Slowenien, Tschechien und Ungarn.

[78] apg.at.

5.2.1 Regulierung

E-Control und RTR als wichtige Player

Der Strommarkt wird in Österreich von der Aufsichtsbehörde E-Control geregelt. Die E-Control gibt u. a. technische und organisatorische Regeln für Netzbetreiber vor, um vor Großstörungen zu schützen bzw. deren Auswirkungen einzugrenzen.[79] Diese Regeln beinhalten unter anderem Schutzvorkehrungen zum Erkennen und Vorbeugen von Spannungs- und Frequenzstörungen. Die Rundfunk- und Telekom Regulierungs-GmbH (RTR[80]) ist für eine Reihe von Regulierungsaufgaben im Bereich Medien und Telekommunikation zuständig. Darunter fallen auch Aspekte der Sicherheit und Integrität von Kommunikationsnetzen für Betreiber (gemäß des Telekommunikationsgesetzes). Für die Schaffung von Standards und Normen unterschiedlicher Art ist das Österreichische Normungsinstitut (Austrian Standards[81]) zuständig.

5.2.2 IT-Notfall Management und Cyber-Sicherheit

Computer Emergency Response Team [CERT] als primäre Anlaufstelle

Das nationale Computer Emergency Response Team (CERT[82]) ist die primäre Anlaufstelle für IT-Sicherheit in Österreich. Es stellt Informationen zu aktuellen Sicherheitslücken und IT-Sicherheit für KMUs bereit, fungiert als Beratungs- und Vermittlungsinstanz zwischen anderen CERTs und übernimmt koordinative Aufgaben bei Angriffen auf nationale IT-Systeme, etwa durch Kommunikation mit Netzbetreibern und zuständigen Sicherheitsteams. Seit 2008 betreibt es auch das vom Bundeskanzleramt initiierte GovCert[83], das sektorspezifische CERT der öffentlichen Verwaltung. Das nationale CERT ist auch Mitglied des CERT-Verbunds, dem verschiedene Branchen und öffentliche Stellen angehören (etwa aus öffentlichen und privaten Rechenzentren, Militär[84], Banken und Versicherungen, Telekombetreiber, etc.). Zur Erhöhung der Cyber-Sicherheit finden auch Übungen und Planspiele für IT-Notfälle (auch im Europäischen Kontext) statt, die vom Bundeskanzleramt bzw. dem BMLVS koordiniert werden. Zur besseren Koordination des Bereichs Cyber-Sicherheit werden seit 2014 die Rahmenbedingungen für ein Cyber Security Center geschaffen, das 2015 in Probebetrieb ging und mit Ende 2017 in operativen Vollbetrieb gehen soll (BKA 2016).

---

79 e-control.at/de/recht/marktregeln/tor.

80 rtr.at.

81 shop.austrian-standards.at.

82 cert.at.

83 govcert.gv.at.

84 Das MilCERT befasst sich vor allem mit der Abwehr digitaler Bedrohungen im Sinne der Landesverteidigung. Eine grundsätzliche Zuständigkeit des Bundesheeres ergibt sich bei Cyber-Angriffen aus Intensität und Intention: Erst wenn die Souveränität der Republik Österreich in Gefahr ist, entsteht eine primäre Zuständigkeit des Heeres. Bis dahin kann die Koordination auf Anfrage (Assistenzeinsatz) oder bei Ausfall/Handlungsunfähigkeit des BMI übernommen werden. Derzeit ist auch das Cyber-Sicherheitsgesetz in Arbeit, das neben anderen Materien die Kompetenzaufteilung zwischen BMI und BMLVS regeln soll: bmi.gv.at/cms/bmi_presse/_news/bmi.aspx?id=6B6C5A6A674C61434172733D&page=0&view=1.

Interessensverbände

Bunte Vielfalt an Initiativen

Neben den staatlich zuständigen Stellen, die mit SKKM und APCIP betraut sind, gibt es einige Interessensverbände und Plattformen, die sich mit den Themen Sicherheit, Cybersecurity, Resilienz und dem Schutz kritischer Infrastrukturen befassen. Mitglieder kommen hier meist aus öffentlichen und privaten Organisationen. Neben der von der Republik Österreich initiierten Cyber-Security Plattform[85], dem IKT-Sicherheitsportal[86], und dem Zentrum für sichere Informationstechnologie (A-SIT[87]), sind das unter anderem das Kuratorium Sicheres Österreich (KSÖ)[88], der Verein Cyber Security Austria[89] (nicht zu verwechseln mit der genannten Plattform), das Resilienznetzwerk Austria[90], das Systemic Foresight Institute[91], sowie die zivilgesellschaftliche Initiative „Plötzlich Blackout!“[92].

Forschung

KIRAS – das österreichische Sicherheitsforschungsprogramm

Im Bereich Forschung gibt es zum Schutz kritischer Infrastrukturen vielfältige Betätigungsfelder. Die Wichtigkeit von Wissenschaft und Forschung wird auch explizit in den verschiedenen nationalen Strategien betont. Von hoher Relevanz in Österreich ist das von BMVIT und FFG ausgeschriebene KIRAS-Programm[93], das nationale Sicherheitsforschung fördert und unter anderem die Einbindung von Bedarfsträgern zum Ziel hat. KIRAS ist ein wichtiger Eckpfeiler der Sicherheitsforschung in Österreich, der wesentlich zur Bewusstseinsbildung und Erforschung sicherheitsrelevanter Themen beiträgt. Die Schwerpunktsetzung des aktuellen Programms liegt auf dem Schutz kritischer Infrastrukturen. Es gibt einige Forschungseinrichtungen mit Schwerpunkt Sicherheitsforschung, wie etwa das Safety & Security Department des Austrian Institute of Technology (AIT), das sich seit mehreren Jahren mit IKT-Sicherheit befasst. Weitere relevante Einrichtungen mit Bezug zu technischen Anwendungen sind etwa die Fachhochschulen St. Pölten und Hagenberg, oder SBA Research. Neben diesen „einschlägigen“ Institutionen ist im breiteren Kontext auch die Zentralanstalt für Meteorologie und Geodynamik (ZAMG) zu erwähnen, die sich u. a. mit der Messung geomagnetischer Aktivität befasst und Informationen zur Erforschung der Wechselwirkungen zwischen Erd- und Solarmagnetaktivität bereitstellt. Darüber hinaus werden auch Erdbebengefährdungszonen definiert, und Wetterwarnungen ausgegeben. Zur Aufbereitung und Veröffentlichung der Daten über Solaraktivität kooperiert die ZAMG mit

Einschlägige Forschungsinstitute aber auch Meteorologie und Weltraumforschung

85 digitales.oesterreich.gv.at/cyber-sicherheit-plattform.

86 onlinesicherheit.gv.at.

87 a-sit.at.

88 kuratorium-sicheres-oesterreich.at.

89 cybersecurityaustria.at.

90 resilienznetzwerk.at.

91 systemicforesightinstitute.org.

92 herbert.saurugg.net/strom-blackout/initiative-ploetzlich-blackout.

93 kiras.at/home.

ESA und NASA. Das ÖAW-Institut für Weltraumforschung (IWF)[94] in Graz befasst sich mit der Erforschung des Sonnensystems im Feld der Physik, entwickelt selbst Weltraumsysteme und ist kontinuierlich an internationalen Weltraumissionen beteiligt. An der Österreichischen Akademie der Wissenschaften beschäftigt sich auch das Institut für Technikfolgen-Abschätzung (ITA)[95] u. a. auch mit den gesellschaftlichen Folgen der Implementierung von Sicherheitstechnologien.

ÖAW: IWF und ITA

5.3 Österreichs Programm zum Schutz kritischer Infrastrukturen (APCIP)

In Kooperation zwischen Bundeskanzleramt und Bundesministerium für Inneres wurde Ende 2014 das Österreichische Programm zum Schutz Kritischer Infrastrukturen beschlossen. Ziel dieses Programms ist es, die Sicherheit und Resilienz kritischer Infrastrukturen in Österreich zu stärken. Zur Zielerreichung sind folgende Prinzipien vorgesehen (BKA 2015, 8):

APCIP Prinzipien

- *„Operator based approach":* Es wird bewusst darauf verzichtet, kritische Sektoren aufzulisten, da die Zusammenhänge zwischen den Sektoren durch die Komplexität nicht abbildbar sind. Österreich orientiert sich stattdessen bei der Identifizierung kritischer Infrastrukturen auf Betreiber strategischer Unternehmen.
- *Subsidiaritätsprinzip und Selbstverpflichtung der Unternehmen:* Österreich setzt auf wechselseitige Verantwortung: Der Staat sieht sich für die Gestaltung der Rahmenbedingungen verantwortlich, um ein besseres Schutzniveau von KI zu erreichen. Unternehmen und Betreiber sind aber primär selbst für den Schutz ihrer Anlagen und Einrichtungen zuständig. Branchenspezifische Schutzstandards sollen hierbei helfen, die Resilienz zu erhöhen.
- *Komplementarität*: Bereits bestehende Maßnahmen und Pläne sollen genutzt und bei Bedarf neuen Bedrohungen angepasst werden.
- *Vertraulichkeit:* Informationen sollen vertraulich und anlassbezogen ausgetauscht werden.
- *Kooperation:* Für die Umsetzung und Weiterentwicklung des APCIP wird auf die Zusammenarbeit aller Stakeholder (Unternehmen und Interessensverbände, öffentliche Verwaltung und Regulatoren, Normungsinstitute und Medien) gesetzt.
- *Verhältnismäßigkeit:* Die mit der Erhöhung des Schutzniveaus verbundenen Maßnahmen und Kosten müssen in einem ausgewogenen Verhältnis zum jeweiligen Risiko stehen.

94 iwf.oeaw.ac.at.

95 www.oeaw.ac.at/ita.

- *All-Hazards-Ansatz:* Maßnahmen zum Schutz kritischer Infrastrukturen sollen auf ein breites Spektrum möglicher Risiken abzielen und nicht punktuell auf einzelne Gefahren.

Ziel: Erhöhung der Resilienz strategisch wichtiger Unternehmen

Ein zentrales strategisches Ziel ist die Erhöhung der Resilienz strategisch wichtiger Unternehmen (siehe unten). Diese Unternehmen sind daher im Rahmen des APCIP aufgefordert, Risikoanalysen durchzuführen, um über ihre eigene Verwundbarkeit in Kenntnis zu sein und risikomindernde Maßnahmen zu setzen. Mittels Krisen- und Sicherheitsmanagement sollen Unternehmen in der Lage sein, Störungen und Notfälle zu überwinden, im Sinne eines Business Continuity Managements, also einer Sichtweise auf Unternehmensprozesse, die Schutz bzw. Umgang mit Krisenfällen laufend mitberücksichtigt. Damit soll die Resilienz Österreichs insgesamt erhöht werden, um die Daseinsvorsorge und die Attraktivität des Wirtschaftsstandorts zu gewährleisten.

Österreich hat wie andere EU-Mitgliedstaaten auf Basis der EKI-Richtlinie eine Liste kritischer Infrastrukturen (ACI – Austrian Critical Infrastructures) und strategisch wichtiger Unternehmen erstellt. Diese Liste ist aufgrund ihrer Sensibilität nicht öffentlich zugänglich. Pschikal (2015) bietet eine Übersicht zu den Kategorien (denen jeweils relevante Unternehmen zugeordnet sind) die hier nur exemplarisch angeführt werden:

Liste kritischer Infrastrukturen

- Land- und Forstwirtschaft, Fischerei
- Bergbau und Gewinnung von Steinen und Erden
- Herstellung von Waren
- Energieversorgung
- Wasserversorgung, Abwasser- u. Abfallentsorgung
- Handel, Instandhaltung und Reparatur von Kraftfahrzeugen
- Verkehr und Lagerhaltung
- Information und Kommunikation
- Finanz- und Versicherungsdienstleistungen
- Wissenschaftliche und technische Dienstleistungen
- Öffentliche Verwaltung, Verteidigung, Sozialversicherung
- Gesundheits- und Sozialwesen

Bei der Auswahl und Priorisierung, welche Unternehmen als strategisch relevant eingestuft werden, sind u. a. die Kriterien Redundanz (wie redundant ist die Leistung einer Unternehmensklasse, gibt es noch andere Unternehmen mit ähnlicher Leistung), Umsatz („too big to fail“) und Mitarbeiteranzahl nach dem Pareto-Prinzip (d. h. jene Unternehmen die 80 % des Umsatzes der strategisch wichtigen Klasse erbringen bzw. jene Unternehmen, die 80 % der Mitarbeiter der strategisch wichtigen Klasse beschäftigen) (Pschikal 2015).

EKI-Richtlinie der Europäischen Union als Basis

Der österreichische Aktionsplan orientiert sich auch stark an der *EKI-Richtlinie* der Europäischen Union. Die Richtlinie bezweckt primär den Schutz vor terroristischen Bedrohungen zu verbessern. Für den Schutz von KI sind laut Richtlinie in erster Linie die Mitgliedstaaten und die Eigentümer bzw. Betreiber kritischer Infrastrukturen verantwortlich. Die Richtlinie sieht allge-

meine Maßnahmen der Mitgliedstaaten vor, um KI zu ermitteln und Sicherheitsvorkehrungen zu treffen. In jedem Land sollten Sicherheitspläne für KI-Anlagen vorhanden sein bzw. bei Fehlen dementsprechende Maßnahmen gesetzt werden. Die Mindestanforderungen an Sicherheitspläne sehen die Nennung der wichtigsten Anlagen, eine Risikoanalyse der wichtigsten Bedrohungen und das Festlegen von Abwehrmaßnahmen (z. B. technische und organisatorische Sicherheitsvorkehrungen, weitgehend im Ermessen des Betreibers) vor. Für die Kommunikation zwischen Infrastrukturbetreibern und zuständigen Behörden sind jeweils Sicherheitsbeauftragte vorgesehen, die es zu ernennen gilt. Zudem ist auch die Weitergabe von Lagebildern durch BMI und BKA an strategische Unternehmen im APCIP vorgesehen.

5.4 Wesentliche Maßnahmen für mehr Resilienz

Resilienz kann verstanden werden als „a system's ability to bounce back to a reference state after a disturbance and the capacity of a system to maintain certain structures and functions despite disturbance" (Turner et al., 2003, S. 8075). Die Stärkung von Resilienz erfordert demnach einerseits bessere Absicherung vor Schadensfällen (etwa durch Vorsorge, Frühwarnung und Foresight), andererseits effektives Krisenmanagement, um funktionsfähig zu bleiben und negative Auswirkungen rasch bewältigen zu können. Die unterschiedlichen Risiken sollten nicht den Blick darauf verstellen, dass die Vorgangsweise im Krisenfall jeweils ähnliche Handlungen erfordert. Hier kann zum Teil auf Erfahrungen aus größeren Stromausfällen und entsprechenden Maßnahmen zurückgegriffen werden. Im Grunde erfordert der Systemausfall durch EMP die gleichen Maßnahmen wie bei einer sonstigen Störung, sofern keine wesentlichen Netzkomponenten beschädigt werden. In Bezug auf Blackout als eine der zentralen Gefahren liegt ein Lernen aus größeren Stromausfällen der Vergangenheit nahe[96]. Hier existiert bei einigen Akteuren Wissen, das auch für andere Akteure relevant sein kann. Eine gemeinsame Wissensbasis, wie sie im APCIP vorgesehen ist, erscheint daher zielführend.

Stärkung von Resilienz

Gemeinsame Wissensbasis wünschenswert

Für das Ziel, die Resilienz kritische Infrastrukturen zu erhöhen, ist in den jeweiligen Sektoren und strategischen Unternehmen eine Reihe von Maßnahmen im Detail erforderlich. Eine wesentliche Gemeinsamkeit ist hierbei die Notwendigkeit von Metasystem- und Prozesswissen zu Struktur- und Ablauforganisation der KI-Bereiche (siehe Abschnitt 4). Ein solches Wissen ist i.d.R. zumindest implizit in Organisationen vorhanden. Bei einem KI-System, das im Schadensfall einen hohen Koordinationseinsatz verschiedener Akteure erfordert, ist allerdings nicht davon auszugehen, dass ein solches Wissen allen handelnden Personen geläufig ist. Dieser Aspekt ist jedoch wichtig, um die Resilienz erhöhen zu können.

Metasystem- und Prozesswissen zu Struktur- und Ablauforganisation essentiell

[96] Z. B. de.wikipedia.org/wiki/Liste_historischer_Stromausf%C3%A4lle.

Das legt nahe, wie oben skizziert, die strategischen Programme und Maßnahmenpakete verstärkt auch integrativ zu betrachten und deren Schnittmengen und Unterschiede klarer zu definieren. Eine Klärung wesentlicher Ansätze (inklusive zentraler Begriffe) in den jeweiligen Kontexten (z. B. gibt es kein einheitliches Verständnis, inwieweit und unter welchen Bedingungen ein Ereignis als Krise, Katastrophe oder Notfall etc. gilt) und Wissen um Indikatoren und Benchmarks zur Differenzierung kann das Zusammenspiel verschiedener Akteure erleichtern. Während einschlägige ExpertInnen in den zuständigen Ministerien i.d.R. über dieses Wissen verfügen, ist aufgrund der Breite des Spektrums kritischer Infrastrukturen jedoch nicht bei allen Akteuren davon auszugehen, dass derartiges Wissen vorhanden ist. Für diese Differenzierung und Präzisierung sind Standards[97] wesentlich wie etwa ÖNORM S 2304 „Integriertes Katastrophenmanagement – Benennungen und Definitionen" die wesentliche Begriffe des KKM definiert.[98] Oder ÖNORM S 2300 für Risiko-, Sicherheits- und Krisenmanagement.[99] In Bezug auf IKT-bedingte Risiken gibt es zudem Bedarf an IT-Expertise und IT-Prozesswissen, um im Notfall rascher mit Ausfällen umgehen zu können.[100] Wichtig ist ein gemeinsames Basis-Wissen und Verständnis in und zwischen den relevanten Akteuren und insbesondere bei KI-Betreibern und strategischen Unternehmen, wo ein solches Wissen nicht ohne weiteres vorausgesetzt werden kann.

Standards als zentrale Instrumente zur Vereinheitlichung von Wissen

Eine Identifizierung der bestehenden Standards, die im Themenkomplex kritischer Infrastruktur relevant sind, erscheint wichtig. Insofern ist die im Rahmen der Plattform Cyber-Sicherheit eingerichtete Arbeitsgruppe für Standardisierung ein begrüßenswerter Schritt. In weiterer Folge ist auch eine Überprüfung der Anwendbarkeit bzw. des Bedarfs zur Anpassung bestehender Standards seitens der zuständigen staatlichen Stellen in Betracht zu ziehen. Abseits der für KKM wichtigen Standards empfiehlt sich auch eine Untersuchung von Sicherheitsstandards für Systeme kritischer Infrastrukturen. Bezüglich EMP-Schutz betrifft das etwa Richtlinien für die elektromagnetische Verträglichkeit (EMV), um Störungen von Geräten und Systemen durch elektromagnetische Felder zu vermeiden. Für die geplante Schaffung der gesetzlichen Rahmenbedingungen zur Erhöhung der

---

[97] Vgl. austrian-standards.at/infopedia-themencenter/infopedia-artikel/katastrophen-praevention-und-hilfe/.

[98] Als Katastrophe gilt etwa ein „Ereignis, bei dem Leben oder Gesundheit einer Vielzahl von Menschen, die Umwelt oder bedeutende Sachwerte in außergewöhnlichem Ausmaß gefährdet oder geschädigt werden und die Abwehr oder Bekämpfung der Gefahr oder des Schadens einen durch eine Behörde koordinierten Einsatz der dafür notwendigen Kräfte und Mittel erfordert."

[99] Etwa eine Differenzierung zwischen Störung (Betrieb beeinträchtigt, behebbar und geringer Schaden), Notfall (Betrieb nicht mehr möglich, bzw. massiv beeinträchtigt und hoher Schaden), Krise (Abweichung vom Normalzustand, längerfristig, mit Bedrohung der Sicherheit (z. B. durch Störung, die nicht mehr in definiertem Zeitraum behebbar und daher auf eine andere Eskalationsebene gelangt).

[100] Eine Einbeziehung von Standards im Bereich IT-Prozesse wie etwa ITIL (IT Infrastructure Library) kann hier überlegenswert sein.

Cyber-Sicherheit[101] empfiehlt es sich, IKT-Abhängigkeiten zu berücksichtigen, um mittel- und längerfristig die Sicherheit zu erhöhen. Das betrifft auch die Forschungsförderung, etwa für die Entwicklung nachhaltigerer Schutzkonzepte, die Systemredundanzen in kritischen Komponenten im Design vorsehen (Security-by-design), wie z. B. die Verwendung von Verschlüsselung zur Entkopplung von Systemen, um der Hyperkonnektivität entgegenzuwirken, ohne die Vorteile zu reduzieren etc.

Neben dem begrifflichen Wissen sind Unterschiede bzw. das Fehlen von konzeptuellem Wissen im Umgang mit Ausfällen bzw. Risiken ein weiterer Aspekt. Im Rahmen des APCIP wurde deshalb ein Handbuch für KI-Betreiber und Unternehmen erarbeitet. Derartige Informationen sind sehr nützlich, um die Maßnahmenkoordination seitens der zuständigen Stellen zu erleichtern. Kritische Infrastrukturen haben i.d.R. eine netzwerkartige Struktur. Wissen über diese Netzwerkstrukturen, etwa in Form von Netzplänen, spielt eine zentrale Rolle, um neuralgische Punkte identifizieren und schützen zu können. Auch die Zuständigkeiten zwischen den verschiedenen Stellen, die mit KI-Schutz betraut sind, scheinen nicht in jedem Fall eindeutig geklärt zu sein. Hierbei ist auch Wissen über Konzepte und Kompetenzen zwischen den Gebietskörperschaften und deren Anwendbarkeit bei größeren Ausfällen von Bedeutung. Das Durchführen von Tests und Übungen (wie in einigen Programmen vorgesehen) ist sehr wichtig und sollte in Zukunft forciert werden.

Gemeinsame Übungen vertiefen notwendiges Kompetenz- und Netzwerkwissen

Wie in Abschnitt 2.2 erläutert, ist Redundanz ein wichtiger Faktor der Bewältigungskapazität, deren Fehlen die Abhängigkeitsproblematik verschärfen kann. Das betrifft sowohl technische als auch organisatorische Aspekte. Für letztere ist etwa die Kooperation und Vernetzung der Akteure des Krisenmanagements und Betreiber kritischer Infrastrukturen ein maßgeblicher Faktor, um Krisen rasch bewältigen zu können, etwa durch klar definierte Zuständigkeiten und Meldeketten. Das betrifft nicht nur die Krisenkommunikation, sondern auch die Bewältigungskapazität innerhalb kritischer Infrastrukturen. Ein weiterer Aspekt ist die Substituierbarkeit der Funktion und Leistungserbringung einer kritischen Infrastruktur im Krisenfall (also inwieweit eine Leistung etwa auch durch einen anderen Betreiber erfolgen kann oder nicht). Damit verbunden ist die Verfügbarkeit von Notfallressourcen wie Notstromaggregaten, notbetriebsfähigen Systemen für die Krisenbewältigung und Mitteln zur Krisenkommunikation. Hinsichtlich der Versorgung mit beispielsweise Treibstoff (aber auch Lebensmittel und Trinkwasser), gehen einige Experten davon aus, dass es bei Ernstfällen (großflächiger und/oder langer Ausfall) zu erheblichen Engpässen kommen kann. Die zuständigen Ministerien (vor allem das BMI) sind eigenen Angaben zufolge bis zu zwei Wochen notbetriebsfähig. Das gilt nicht für zivile Einrichtungen, hier besteht weitgehend Unklarheit darüber, welche Einrichtungen über Notstromaggregate verfügen bzw. über die Menge an

Redundanz und Substitutionsfähigkeit erhöhen Bewältigungskapazität

Allerdings ist unklar, wie hoch diese in verschiedenen Bereichen ist

[101] An einem Gesetzesvorhaben wird derzeit gearbeitet: kuratorium-sicheres-oesterreich.at/allgemein/ksoe-rechts-und-technologiedialog-zur-cybersicherheit/.

vorrätigem und verwendbarem Diesel-/Heizöltreibstoff. Hier gibt es weiteren Klärungsbedarf, um einerseits Notressourcen im Bedarfsfall zur Verfügung zu haben, bzw. deren Beschaffung zeitgerecht zu koordinieren (etwa durch Kooperationen und Hilfseinsätze mit dem Ausland). Andererseits, um Eigenschutz und Selbstorganisationsfähigkeit in der Zivilgesellschaft zu fördern.

Information und Kommunikation sind essentiell, um Krisen bewältigen zu können. Redundanzmängel können hier fatale Folgen haben. Das betrifft zum einen das Vorhandensein von Kommunikationsmitteln zum anderen auch deren Funktionsfähigkeit im Krisenfall. In Anbetracht der genannten Ausfallrisiken besteht hier eventuell Bedarf, als krisensicher geltende Systeme auf Nutzbarkeit zu überprüfen bzw. bei Bedarf umzurüsten. Neben den komplexen EMP-Risiken ist das vor allem aufgrund der hohen IKT-Abhängigkeit zweckmäßig, um hier Krisenfestigkeit zu gewährleisten und Alternativ-Systeme, die weniger störanfällig sind, für den Krisenfall verfügbar zu halten. Hierbei spielt insbesondere auch der Analog-Funk eine wichtige Rolle, um auch bei Ausfall der herkömmlichen Kommunikationsinfrastruktur (Telefon, Internet etc.) handlungsfähig zu bleiben. Das betrifft grundsätzlich alle relevanten Akteure des Krisenmanagements und insbesondere staatliche Stellen und Betreiber kritischer Infrastrukturen. Aber auch eine Einbeziehung von ehrenamtlichen Einrichtungen und Organisationen der Zivilgesellschaft etwa von Amateurfunkverbänden o.dgl. kann hier sehr sinnvoll sein. Aufgrund von IKT-Abhängigkeiten und der steigenden Verbreitung von digitalen Funksystemen empfiehlt sich auch hier eine Überprüfung. Gleiches gilt für satellitenbasierte Navigationssysteme. Zudem ist das Wissen über Krisenkommunikationsabläufe und die Priorisierung der Nutzung der einzelnen Systeme relevant. Laut ExpertInnen existiert etwa auch ein kupferleitungsbasiertes Kommunikationsnetz das alle Ministerien, das BKA, alle Kasernen und alle Bezirkshauptmannschaften verbindet bzw. verband. Das Netz wurde vor ca. 30 Jahren, zur Zeit des Kalten Krieges installiert und ist heute praktisch ungenützt. Die Leitungen (physikalisch) wären aber noch vorhanden. Je nach Art der Katastrophe könnte das auch zur Kommunikation verwendet werden.

Analog-Funk als Notfalltechnologie

Nicht zuletzt ist vor allem auch die Information und Kommunikation mit der Bevölkerung zentral, um Panik zu vermeiden und die Selbstorganisation und Resilienz in der Bevölkerung und des Einzelnen zu stärken. In Summe bedarf es insbesondere eines akkordierten Dreiklangs von Redundanz, Resilienz und Selbstorganisation in staatlichen Stellen, KI-Betreibern und Zivilgesellschaft, um die Vulnerabilität kritischer Infrastrukturen gesamtheitlich zu reduzieren.

6 Zentrale Herausforderungen und Empfehlungen

Wie obige Ausführungen zeigen, gibt es eine Reihe von Herausforderungen beim Schutz kritischer Infrastrukturen. Diese resultieren zum einen aus der hohen Komplexität moderner Infrastruktursysteme, die zwar mit Gefahren, die nur bedingt neu sind, konfrontiert sind, für die jedoch heute andere Rahmenbedingungen gelten als vor der Digitalisierung. Dadurch ergeben sich auch zumindest teilweise veränderte Anforderungen an die Risikobewertung. Eine Bewertung von Einzelbereichen ist durch die hohe Integration von Teilbereichen und die digitale Vernetzung zunehmend erschwert. Im Folgenden werden zusammenfassend die wichtigen Herausforderungen und Empfehlungen dargestellt, die im Rahmen dieser Studie erarbeitet wurden.

Komplexe Risiken mit potenziell hohem gesellschaftlichem Schaden

Die in dieser Studie untersuchten Risiken haben eine eher geringe Eintrittswahrscheinlichkeit, bei Eintritt der Ereignisse führen sie aber potenziell zu hohem gesellschaftlichen Schaden. Gefahren wie EMPs und Solarstürme sind zwar keine unbekannten Größen, aufgrund der Vielzahl heute schon vernetzter Technologien ist aber mit größeren Störungspotenzialen zu rechnen. Daher ist trotz geringer Eintrittswahrscheinlichkeit mehr Bewusstsein für die Problematik notwendig. Zudem erscheint die Identifizierung etwaiger Schwachstellen bezüglich elektromagnetischer Verträglichkeit in strategisch wichtigen Bereichen sinnvoll.[102]

Geringe Eintrittswahrscheinlichkeit

Da (N)EMPs (wie in Abschnitt 3.1 erläutert) militärische Ressourcen und Aktivitäten voraussetzen, ergeben sich für Österreich (auch aufgrund seiner geopolitischen Lage und Neutralität) zwar keine besonderen Herausforderungen, was den Einsatz von Nuklearmaterial betrifft. Derartige Gefahren sind vor allem Gegenstand der militärischen Landesverteidigung.

aber Forschungsbedarf hinsichtlich

Allerdings erscheint eine Berücksichtigung unterschiedlicher EMP-Risiken für den Schutz kritischer Infrastrukturen insgesamt dennoch sinnvoll, da die potenziellen Auswirkungen auf moderne Infrastrukturen heute andere sind, als etwa in den 1960er Jahren. Zudem ergeben sich mit der Möglichkeit von HPM-Waffen neue Bedrohungen, die zwar verglichen mit NEMPs geringeren, aber dafür gezielteren Schaden anrichten können.

Auswirkungen und Vorhersage

Über die Entstehung von EMPs durch Weltraumwetterphänomene wie Solarstürme (die weitgehend EMPs des Typs E3 entsprechen) und deren Auswirkungen auf der Erde ist noch relativ wenig bekannt. Hier besteht international weiterer Forschungsbedarf, um derartige Ereignisse besser verstehen zu

[102] Das gilt auch für Innovationen, bei denen frühzeitig derartige Risiken berücksichtigt werden sollten. Ein Beispiel sind neuartige Transformatoren zur Geräuschreduktion elektromagnetischer Interferenzen ("ultralow noise transformers" bzw. „Flüster-Trafo"). Interviewpartnern zufolge können diese je nach Design anfälliger für EMPs sein, da sie mit anderer Spannung arbeiten.

können, nicht zuletzt auch hinsichtlich ihrer Bedeutung bei steigender Vernetzung und Systemabhängigkeit.[103] Zentral ist hierbei auch die Verbesserung von Frühwarnsystemen und Forecasting, besonders im Bereich von Geomagnetik und Solaraktivitäten, sowie deren Auswirkungen.

Forschung zu EMP-Schutz und EMV in komplexen Systemen

Auch über die tatsächlichen Gefährdungen durch EMP sowie der Wirksamkeit von Schutzvorkehrungen (EMP-Schutz und elektromagnetische Verträglichkeit (EMV), ist bislang wenig bekannt. Zwar existieren seit langem Vorgaben für EMV, inwieweit diese aber auch vor komplexen Risiken durch starke EMPs schützen, bedarf genauerer Detailanalysen in spezifischen KI-Bereichen. In weiterer Folge können dann Schutzmaßnahmen entwickelt bzw. erweitert werden. Das bedeutet nicht unbedingt, sämtliche KI-Systeme mit EMP-Schutz zu versehen. Vielmehr können hier, sofern tatsächlich dementsprechende Vulnerabilität festgestellt wurde, kritische Komponenten und Netzknotenpunkte (wie etwa Transformatoren und daran gekoppelte Schnittstellen) nachgerüstet werden (vgl. Baker 2015). Derartige Investitionen im Stromnetz als Art „Hauptschlagader" kritischer Infrastrukturen können insgesamt deren Resilienz erhöhen. Österreich scheint zwar durch seine Lage weniger gefährdet als die USA oder Skandinavien.[104] Dennoch gibt es Bedarf nach mehr Wissen über diese Problematik, um mehr Klarheit über die tatsächliche Gefahrenlage und die Notwendigkeit von Investitionen zu erlangen. Hier können Erfahrungen anderer Ländern, die stärker von geomagnetischen Phänomenen betroffen sind, genutzt werden. Beispielsweise wurden in Schweden Transformatoren umgerüstet[105] und mit einem wirksameren Überspannungsschutz ausgestattet. Eine Fortführung bzw. Stärkung von Forschungskooperationen Österreichs erscheint beim globalen Phänomen Weltraumwetter jedenfalls sinnvoll. Zumal sich zeigt, dass es sich dabei um eine auch für ganz Europa relevante Thematik handelt. Auf europäischer wie auch nationaler Ebene besteht Bedarf nach Überprüfung und gegebenenfalls Anpassung von Richtlinien zur elektromagnetischen Verträglichkeit (EMV).[106]

Inventarisierung kritischer Komponenten

Teilweise Nachrüstung

Internationale Forschungskooperationen

[103] Dieser Bedarf spiegelt sich u. a. in Initiativen der USA und Großbritannien wider, die jeweils eigene nationale Strategien zu Weltraumwetterphänomenen entwickelt haben (UK Gov 2015, NSTC 2015).

[104] Naturgefahren wie Muren, Lawinen und Hochwasser sind hierzulande eher präsent.

[105] abb.com/cawp/seitp202/c99eb3b89c85b7b2c12571c6004579aa.aspx.

[106] In Österreich sind vor allem Wirtschaftsministerium und E-Control mit EMV-Richtlinien betraut.

Vernetzung, Schnittstellen und Systemabhängigkeiten erfordern neue Ansätze

Kaskadeneffekte erhöhen Schadenspotentiale

Wie in Abschnitt 4 ausgeführt, liegt eine Kernproblematik beim Schutz kritischer Infrastrukturen (weitgehend unabhängig von den jeweiligen Ausfallrisiken) in den Abhängigkeiten zwischen KI-Systemen. Ausfälle können zu Kaskadeneffekten führen und andere Netze beeinträchtigen. Technische Abhängigkeiten zu verschiedenen IKT-Systemen sind hierbei ein zentraler Aspekt. Ansätze, um diese Problematik zu reduzieren, sind nur in geringem Ausmaß vorhanden. Es ist wenig bekannt, in welchen Bereichen und welche Komponenten von KI-Systemen durch IKT besonders gefährdet sind. Dementsprechend gibt es insgesamt Bedarf nach einer stärkeren Berücksichtigung von Abhängigkeiten zwischen und innerhalb kritischer Infrastruktursysteme. Das betrifft einerseits die Bewusstseinsbildung bei allen Akteuren insbesondere in Politik und Verwaltung und KI-Betreibern. Andererseits besteht Bedarf nach Erarbeitung konkreter Schutz-Maßnahmen vor Abhängigkeiten.

Verstärktes Bewusstsein für Abhängigkeiten notwendig

Mehr inter- und transdisziplinären Austausch

Kaskadeneffekte können größere Folgeschäden auslösen, was dem zugrundeliegenden Problem höhere Brisanz verleiht. Insofern besteht Bedarf nach mehr IT-Expertise für den Schutz kritischer Infrastrukturen sowie für mehr inter- und transdisziplinären Austausch, um mehr Wissen über die Unterschiede und Gemeinsamkeiten von Energie- und IKT-Netzen zu erlangen. Bezüglich technischer Entwicklungen und Innovation gibt es mittel- und längerfristig Bedarf nach Ansätzen, die die Systemsicherheit im Design bzw. der Architektur erhöhen (Security by design).

Vorausschauendes Security-by-design

IT-Security Expertise gefragt

Schulung und Ausbildung notwendig

Dabei sollten Abhängigkeiten und Schnittstellen besser berücksichtigt und geschützt werden. Das betrifft primär die Technologie-Hersteller, die KI-Betreiber könnten hier aber dementsprechend Bedarf signalisieren und dahingehend von öffentlichen Nachfragern bzw. Fördergebern unterstützt werden. Das gilt für IKT-Komponenten im Allgemeinen, aber insbesondere für solche beim Einsatz in kritischen Infrastrukturen. Insgesamt lässt sich ein steigender Bedarf nach Expertise im Bereich IKT-Sicherheit feststellen, um die zunehmende Integration dieser Systeme in kritische Infrastrukturen besser verstehen und absichern zu können. Entsprechende Ausbildungs- und Schulungsmaßnahmen bei KI-Betreibern erscheinen sinnvoll und können im Rahmen des APCIP und den darin vorgesehenen Sicherheitsbeauftragten umgesetzt werden.

Versteckte Abhängigkeiten durch integrierte Systeme

Zunehmende Vernetzung als Herausforderung

Wie in Kapitel 4.2 gezeigt, liegt eine der zentralen Herausforderungen in der weiteren Zunahme vernetzter Systeme. Für das Zusammenwirken innerhalb und zwischen KI-Systemen sind Schnittstellen erforderlich. Diese fungieren i.d.R. als Kopplungspunkte unterschiedlicher Komponenten und Systeme und können so die Vulnerabilität erhöhen. Die Faustregel lautet „Schnittstellen erhöhen die Komplexität des Systems und machen es somit potenziell anfälliger." In diesem Zusammenhang spielen Netzpläne eine zentrale Rolle, um neuralgische Punkte identifizieren und dann auch schützen zu können. Darin sollten Schnittstellen explizit sichtbar gemacht werden. Zudem ist eine Unterscheidung zwischen internen (innerhalb eines Systems) und externen Schnittstellen (Anbindung externer Systeme) zweckmäßig. Dies vor allem, um „nicht-offensichtliche" Abhängigkeiten erkennen zu können. Ein konkretes Beispiel für eine bislang zu wenig beachtete Abhängigkeit resultiert aus dem Einsatz von GPS und anderen Satellitensystemen. Wie in Abschnitt 4.2 ausgeführt, ist nach derzeitigem Wissensstand auch in Österreich erst wenig über die Integration und die Abhängigkeit kritischer Infrastrukturen von Satellitensystemen (insbesondere GPS) bekannt. GPS-Komponenten werden nicht nur in der geläufigsten Anwendung Navigation eingesetzt, sondern auch in anderen Bereichen z. B. zur Zeitsynchronisation (siehe Abschnitt 4). Das kann z. B. auch bei Umspannwerken im Stromnetz der Fall sein. Die Integration dieser (und anderer) IKT-Systeme in KI ist ein Beispiel für eine bislang eher vernachlässigte System-Abhängigkeit.[107] Bei einem Ausfall können diese Abhängigkeiten ohne verfügbare Alternativsysteme zu massiven Schwierigkeiten führen. Insbesondere dann, wenn Systeme nicht redundant ausgeführt sind und nicht ohne weiteres umrüstbar sind (etwa auf alternative Komponenten zur Navigation oder Zeitsynchronisation). Zudem kann mangelndes Bewusstsein für diese Problematik die Umsetzung von Notfallmaßnahmen bei Ausfällen erschweren.

Netzpläne und Schnittstellendokumentation krisensicher, analog vorhalten

GPS als unterschätztes Risiko

Im Hinblick auf weiter zunehmende Vernetzung und Automatisierung (z. B. Industrie 4.0, Smart Grids, Smart Home, autonome Fahrzeuge, Internet der Dinge etc.) ist davon auszugehen, dass solche Systeme weiter an Bedeutung gewinnen werden. Dies wird Systemabhängigkeiten weiter verschärfen. Es ist daher besonders wichtig, diese und ähnliche Abhängigkeiten, beim Schutz kritischer Infrastrukturen besser zu berücksichtigen. Auf Betreiberseite können betroffene Komponenten und deren Bedeutung für die Funktionsfähigkeit der KI-Systeme identifiziert und gegebenenfalls (bei besonders kritischen Komponenten) nach- bzw. umgerüstet werden.

[107] Neben Satellitensystemen wird etwa auch der Mobilfunkbereich immer stärker in verschiedene Systeme integriert.

Nachdem Schnittstellen neuralgische Punkte sind, die Abhängigkeiten implizieren können, ist deren explizite Berücksichtigung in systematischen Vulnerabilitätsanalysen dringend notwendig. Das gilt vor allem für jene Netzkomponenten, bei deren Ausfall mehr als ein Netzbereich betroffen wäre und die Gefahr von Kaskadeneffekten besteht. So kann die frühzeitige Erkennung bislang unerkannter Gefahren von Kaskadeneffekten unterstützt werden.

Stärkere Beachtung von Schnittstellen

Die Durchführung von Vulnerabilitätsanalysen und gegebenenfalls notwendige Maßnahmen zur Erhöhung des Schutzniveaus kritischer Infrastrukturen sind jedoch mit ökonomischem Aufwand verbunden und können kostspielige Investitionen erfordern. Um wirtschaftlichen Restriktionen zu genügen, empfiehlt es sich, Prioritäten zu setzen. Aufgrund der Kernproblematik – System-Abhängigkeiten und Kaskadeneffekte – ist es hierbei weder nötig noch zweckmäßig, ein gesamtes System umzurüsten. Es erscheint stattdessen sinnvoll, gezielte Schwachstellenanalysen durchzuführen, um kritische Komponenten zu erkennen und diese in Folge, abhängig von Vulnerabilität und Bewältigungskapazität, besser zu schützen.

Schwachstellenanalyse und Priorisierung der Sicherung kritischer Komponenten

Ein weiterer Aspekt der Vernetzungs- und Abhängigkeitsproblematik sind grenzüberschreitende Probleme, wie z. B. im Falle eines Blackouts. Daher ist Krisen- und Katastrophenschutzmanagement auch aus europäischer Ebene zu beachten. Dies erfordert einen geregelten Kommunikationsfluss zwischen Akteuren und KI-Betreibern im europäischen Kontext wofür die EKI-Richtlinie einen Rahmen vorgibt. Diese Aktivitäten sollten fortgeführt werden.

Redundanz und Substituierbarkeit als zentraler Aspekt der Krisenbewältigung

Redundanz ist ein wichtiger Faktor zur Erhöhung der Bewältigungskapazität. Redundanz wird gemeinhin in der mehrfachen Vorhaltung von Systemkomponenten gesehen. Ein modernes Verständnis von Redundanz sollte jedoch auch andere Ressourcen und Aktivitäten umfassen, die auf die Aufrechterhaltung der ursprünglichen Funktionalität abzielen. Dies kann alternative technische oder auch organisatorische Maßnahmen umfassen. Aufgrund ökonomischen Drucks sind redundante Systeme jedoch oftmals nicht vorhanden. Das ist auf längere Sicht eine problematische Entwicklung, die Systemunsicherheiten erhöht. Neben technischen Redundanzen ist auch personelle Redundanz ein maßgeblicher Faktor, um Krisen rasch bewältigen zu können. Dies umfasst klar definierte Zuständigkeiten (inklusive Ausfallvertretung).

Redundanz oft unter ökonomischem Druck

Die Bewältigungskapazität von integrierten Systemen wird auch durch Kooperation und Vernetzung von Akteuren des Krisenmanagements und den Betreibern kritischer Infrastrukturen verbessert. Dies insbesondere, wenn Funktion und Leistungserbringung einer kritischen Infrastruktur im Krisenfall durch andere Betreiber erfolgen kann (Substituierbarkeit).

Substituierbarkeit – Leistung durch andere erbringbar?

Fehlende Redundanz kann auch die Folge einer Krise sein und zum Problem werden. Konkret dann, wenn Redundanzen durch einen Schadensfall außer Funktion gesetzt werden. Das heißt, die Wiederherstellung einer kritischen Infrastruktur umfasst letztlich auch Nachrüstung und Wiederaufbau von Redundanzen, was mit zusätzlichem Kosten- und Ressourcenaufwand verbunden ist. Die Wirksamkeit von Redundanzen bedingt auch Wissen über ihre Verfügbarkeit. Das erscheint zunächst selbstverständlich, im Krisenfall kann allerdings mangelnde Transparenz über existierende bzw. nicht existierende Redundanzen aller Art zusätzliche Probleme bei der Bewältigung verursachen. Die Dokumentation von technischen und organisatorischen Redundanzen in einem KI-System sowie die regelmäßige Wartung redundanter Systemkomponenten sind daher ebenso wichtig.

Österreichs Strategie zum Schutz kritischer Infrastrukturen

Österreichs Strategie zum Schutz kritischer Infrastrukturen verfolgt einen funktionsorientiert-kooperativen Ansatz zwischen Staat und Wirtschaft

In Österreich werden einige Aktivitäten und Initiativen für den Schutz kritischer Infrastrukturen verfolgt, und bei den relevanten Akteuren ist entsprechendes Problembewusstsein vorhanden. Die APCIP Strategie der Österreichischen Bundesregierung orientiert sich an der Europäischen Strategie (in deren Entwicklung Österreich involviert ist). Der gewählte funktionsorientierte Ansatz, der stark auf Kooperation zwischen Behörden und öffentlichen Einrichtungen sowie (privaten) Betreibern kritischer Infrastrukturen setzt, erscheint zweckmäßig, um Sicherheit und Resilienz kritischer Infrastrukturen in Österreich zu stärken. Die APCIP hat ihren Fokus in Abgrenzung zum SKKM auf dem Themenkomplex KI. APCIP versteht sich als Ansatz, der staatliches Krisen- und Katastrophenschutzmanagement (SKKM) nicht ersetzt, sondern erweitert; etwa durch die Entwicklung umfassender Konzepte zum Risiko-, Krisen- und Sicherheitsmanagement. SKKM als gesamtstaatliches Verfahren ist mit der Koordination der Maßnahmen relevanter Akteure zwischen Bund, Ländern und Gemeinden zur Katastrophenprävention, -vorsorge, -hilfe und Maßnahmen zur Schadensbegrenzung betraut. KIs fließen hierbei eher allgemein im Bereich Prävention und Vorsorge mit ein (BKA 2015). Um eine etwaige „Verdopplungsgefahr" zwischen APCIP und SKKM zu vermeiden, sollte auf Synergien zwischen beiden Ansätzen, sowie die Präzisierung der jeweiligen Besonderheiten und Anforderungen (etwa der jeweils unterschiedlichen Beurteilung bzw. Bedeutung von Katastrophen und Krisen) geachtet werden. Eine Analyse (und gegebenenfalls Adaptierung) des Krisen- und Katastrophenschutzmanagements in Hinblick auf APCIP, Überschneidungen, Synergien und Ressourcen erscheint daher zweckmäßig. Gerade weil Österreich einen funktionsorientierten Ansatz verfolgt, der stark auf die Eigenverantwortung der KI-Betreiber setzt, sind Standards im Sicherheitsmanagement bzw. betrieblichen Krisenmanagement besonders relevant. Hierbei sollte evaluiert werden, inwieweit Anpassungsbedarf besteht.

Gemeinsame Standards besonders wichtig

Akteure und Bewusstseinsbildung

In Österreich beschäftigen sich zahlreiche Akteure aus dem öffentlichen und dem privaten Sektor seit mehreren Jahren mit der Thematik. Es existieren Kooperationen in Form von Arbeitsgruppen und Vernetzungsaktivitäten. Die Themen sind teilweise sehr breit gefächert bzw. stark an Angriffs- und Abwehrszenarien im Bereich Cyber-Attacken, Terrorismus etc. orientiert. Das ist zwar ein wichtiger Teilaspekt, allerdings erscheint allgemeine Ursachenbekämpfung und Verbesserung der Systemsicherheit durch Verringerung von Vulnerabilität und Erhöhung der Bewältigungskapazität kritischer Infrastrukturen bisher zu wenig beachtet. Gerade diese Aspekte sind aber wesentlich, um Ausfall- sowie Angriffsrisiken im Vorfeld besser zu fassen und eingrenzen zu können. Trotz der hohen Bedeutung von Cyber-Angriffsszenarien sollten systemimmanente Gefahren wie Systemfehler, abhängigkeitsbedingte Stör- und Ausfälle nicht unterschätzt werden. Dazu kommt, dass es auch Akteure gibt, die bislang kaum einbezogen wurden.

Vielzahl von Akteuren

Insofern besteht Bedarf nach Bewusstseinsbildung, Austausch und Kooperation unter den KI-Betreibern. Die im APCIP vorgesehenen Notfallübungen, um das Zusammenspiel der verschiedenen Akteure zu trainieren, sind wichtig, weil dadurch die Bearbeitung von Szenarien größerer Ausfälle (drei oder mehr Tage) und von Szenarien mit IKT-bedingten Ausfällen ermöglicht wird. Insbesondere sollten auch die Abhängigkeiten verstärkt berücksichtigt werden. Das heißt die Zuständigkeiten und Rollenverteilung zwischen Akteuren bzw. relevanten Institutionen sollte besser nachvollziehbar sein. So sollten Meldeketten bei Blackout klar definiert sein. Wesentlich erscheint auch die Beachtung der europäische Ebene und die Zusammenarbeit und Kommunikation zwischen den Ländern. Kritische Aspekte der Krisenkommunikation können durch mangelnde Interoperabilität und Kompatibilität z. B. durch unterschiedliche Standards der Krisenkommunikation in technischer wie auch organisatorischer Hinsicht entstehen (wie etwa mögliche Unterschiede in Behördenfunksystemen anderer Staaten). Dies kann insbesondere bei Staatsgrenzen überschreitenden Krisen problematisch sein.

Notfallübungen, transparente Zuständigkeiten und Meldeketten

Krisenkommunikation und Notfallressourcen

Um im Ernstfall handlungsfähig zu bleiben, ist aber auch die Offline-Verfügbarkeit von Netzstrukturplänen und Alarmplänen wichtig. Es ist grundsätzlich davon auszugehen, dass die Krisen-Akteure und KI-Betreiber über solche verfügen. Die Verfügbarkeit sollte aber explizit von den jeweiligen Akteuren überprüft und gegebenenfalls nachgerüstet werden. Das bezieht sich vor allem auch auf IKT-Abhängigkeiten im Bereich der Krisenkommunikation. Hier besteht Bedarf Wissen über krisensichere und weniger krisensichere Systeme zu schaffen und die Verfügbarkeit der krisensicheren zu gewährleisten. Bei einem Ausfall informationstechnischer Systeme ist mit Störungen oder Nicht-Verfügbarkeit digitaler Kommunikationsnetze zu rechnen. Um die Kommunikation weiterhin zu ermöglichen, sind Alternati-

ven erforderlich. Als krisenrobustes Kommunikationsmittel gilt insbesondere die Funktechnologie. Es sollte daher die Verfügbarkeit und Nutzbarkeit von Funktechnologie unter allen relevanten Akteuren auch im Krisenfall sichergestellt werden, sodass die Krisenkommunikation zwischen den Akteuren möglichst friktionsfrei funktioniert. Das gilt einerseits für staatliche Einrichtungen, die im Krisenfall zuständig sind als auch für Betreiber kritischer Infrastrukturen. Hier gilt es auch, mehr Transparenz über die Verfügbarkeit staatlicher Krisenkommunikationsmitteln zwischen den Akteuren zu schaffen. Dazu zählen etwa das Fernmeldesystem des Bundesheers (FMSys-ÖBH)[108] oder priorisierte Leitungen für die staatliche Krisenkommunikation (ehemaliges Staatsgrundnetz oder Zivilschutznetz; in der Schweiz wird etwa die Reaktivierung eines solchen angedacht). Für die bessere Koordination erscheint die Errichtung eines gesamtstaatlichen Lagezentrums, wie sie im Regierungsprogramm 2013–2018 vorgesehen ist, sinnvoll, um die nationale Bewältigungskapazität zu erhöhen.

Offline-Verfügbarkeit von Notfallplänen

und

analoge Kommunikationsmittel (Funk)

Für Notversorgung (neben Gütern wie Lebensmittel etc.) ist die Verfügbarkeit von Ressourcen für Energie und Kommunikation essentiell. Im Notfall ist Wissen darüber essentiell, welche Geräte, Komponenten etc. nutzbar sind (z. B. Mobile Sende- und Empfangsstationen, Fahrzeuge etc.). Das betrifft auch Ressourcen zur Notstromversorgung wie Notstromaggregate, die Bedeutung von Akkus und die Dauer der Verfügbarkeit bei begrenzten Laufzeiten etc. Fahrzeuge spielen hierbei eine zentrale Rolle da diese über eine eigene Stromversorgung und unabhängigen Radioempfang verfügen. Für diese Aspekte gilt es auch im Bereich des Zivilschutzes und in der Bevölkerung mehr Bewusstsein zu schaffen. Auch bezüglich der Notversorgung der Bevölkerung gibt es einige offene Fragen. Manche Experten gehen hier von erheblichen Engpässen bei Krisen, die länger als 3 Tage dauern aus. In Summe ist Österreich in vielerlei Hinsicht gut für diverse Krisen und Katastrophen gewappnet. Ein zentraler Aspekt im Ernstfall sind naturgemäß Resilienz und die Selbstorganisationsfähigkeit aller gesellschaftlichen Akteure. Diese gilt es mit Koordination und zeitnaher Bereitstellung von Ressourcen bzw. Möglichkeiten zur Beschaffung zu fördern, sodass die Funktionsfähigkeit der Gesellschaft auch im Krisenfall weitestgehend gewährleistet ist.

Bewusstsein in der Bevölkerung schaffen

[108] bundesheer.at/truppendienst/ausgaben/artikel.php?id=1400.

Literatur

Alle URLs, auch jene in den Fußnoten im Text wurden zuletzt am 23.2.2017 aufgerufen.

Austrian Power Grid AG (APG) (2014): Geschäftsbericht 2014

Baker, G. H. (2015): Joint Hearing on „The EMP Threat: The State of Preparedness against the Threat of an Electromagnetic Pulse (EMP) Event". May 13, 2015, Testimony of George H. Baker Professor Emeritus, James Madison University before the House Committee on National Security and the House Subcommittee on the Interior of the House Committee on Oversight and Government Reform. https://oversight.house.gov/wp-content/uploads/2015/05/Baker-Statement-5-13-EMP.pdf

Baylon, C., Brunt, R., Livingstone, D. (2015): Cyber Security at Civil Nuklear Facilities – Understanding the Risks. Chatham House Report. Royal Institute of International Affairs, London.

BBK – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2006): Bericht über mögliche Gefahren für die Bevölkerung bei Großkatastrophen und im Verteidigungsfall. Schriftenreihe der Schutzkommission beim Bundesminister des Inneren Band 59, Bonn. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenForschung/Band59.html

BDEW – Bundesverband der Energie- und Wasserwirtschaft (2015): Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. Februar 2015, https://www.bdew.de/internet.nsf/id/232E01B4E0C52139C1257A5D00429968/$file/OE-BDEW-Whitepaper_Secure_Systems%20V1.1%202015.pdf

Birkmann, J., Bach, C., Guhl, S., Witting, M., Welle, T., Schmude, M. (2010): State of the Art der Forschung zur Verwundbarkeit kritischer Infrastrukturen

BKA – Bundeskanzleramt (2013a): Österreichische Sicherheitsstrategie, Sicherheit in einer neuen Dekade – Sicherheit gestalten, https://www.bka.gv.at/DocView.axd?CobId=52099

BKA – Bundeskanzleramt (2013b): Österreichische Strategie für Cyber Sicherheit, https://www.digitales.oesterreich.gv.at/at.gv.bka.liferay-app/documents/22124/30428/OesterreichischeStrategieCyber-Sicherheit.pdf/fd94cf23-719b-4ef1-bf75-385080ab2440

BKA – Bundeskanzleramt Österreich (2015): Österreichisches Programm zum Schutz kritischer Infrastrukturen – Masterplan 2014. Jänner 2015, https://www.bka.gv.at/DocView.axd?CobId=58907

BKA – Bundeskanzleramt Österreich (2016): Bericht Cyber Sicherheit 2016. Mai 2016, http://archiv.bundeskanzleramt.at/DocView.axd?CobId=63191

BMI – Bundesministerium für Inneres (2007): Richtlinie für das Führen im Katastropheneinsatz. Erste Auflage Februar 2007. http://www.bmi.gv.at/cms/bmi_service/richtlinie_fuer_das_fuehren_im_katastropheneinsatz.pdf

BMI – Bundesministerium für Inneres (2009): SKKM Strategie 2020 – Staatliches Krisen- und Katastrophenschutzmanagement, Juli 2009, http://www.bmi.gv.at/cms/BMI_Zivilschutz/management/vorsorge/files/006_Fuehren_im_KatEinsatz.pdf

BSI – Bundesamt für Sicherheit in der Informationstechnik (2013): ICS-Security-Kompendium. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile

BSI – Bundesamt für Sicherheit in der Informationstechnik (2014): UP KRITIS: Öffentlich-Private-Partnerschaft zum Schutz Kritischer Infrastrukturen. Grundlagen und Ziele, Bundesamt für Sicherheit in der Informationstechnik Geschäftsstelle UP KRITIS, http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Fortschreibungsdokument.pdf?__blob=publicationFile

Butt, Y. M. (2010): The EMP threat: fact, fiction, and response http://www.thespacereview.com/article/1549/1

Cannon, P. et al (2013): Extreme space weather: impacts on engineered systems and infrastructure. Royal Academy of Engineering, London

Dax, Patrick (2015): Blackout: Wahrscheinlichkeit geringer als vor 10 Jahren, Interview mit E-Control Vorstand Walter Boltz, futurezone 11.9.2015, http://futurezone.at/digital-life/blackout-wahrscheinlichkeit-geringer-als-vor-10-jahren/150.434.517

DC – Defence Committee of the House of Commons (2012): Developing Threats: Electro-Magnetic Pulses (EMP). Tenth Report of Session 2010-12. The House of Commons, London, 22 February 2012

EUC - European Commission (2012): Commission staff working document on the review of the European programme for critical infrastructure protection (EPCIP). Brussels, 22.6.2012 SWD(2012) 190 final

Foster, J. et al (2008): Report of the Commission to assess the threat to the United States from Electromagnetic Pulse (EMP) attack – critical national infrastructures, April 2008

GAO – United States Government Accountability Office (2016): Critical infrastructure protection – Federal Agencies Have Taken Actions to Address Electromagnetic Risks, but Opportunities Exist to Further Assess Risks and Strengthen Collaboration. Report to Congressional Requesters. March, 2016, http://www.gao.gov/assets/680/676030.pdf

Jachs, S. (2014): Staatliches Krisen- und Katastrophenschutzmanagement in Österreich. Vortrag bei 2. BMBF–Innovationsforum „Zivile Sicherheit" Session 1C Krisenmanagement: Aktuelle Forschungsergebnisse – Einführung, Berlin, 07. Mai 2014

Krausmann, E., Andersson, E., Murtagh, W., Mitchison, N. (2013): Space Weather and Power Grids: Findings and Outlook. JRC Scientific and Policy Reports, European Commission 2013

Korreng, M., D. (2011): UTC Time Transfer for High Frequency Trading Using IS-95 CDMA Base Station Transmissions and IEEE-1588 Precision Time Protocol. In: Proceedings of the 42nd annual precise time and time interval (PTTI) meeting.

Lenz, S. (2009): Vulnerabilität Kritischer Infrastrukturen. Forschung im Bevölkerungsschutz Band 4, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bonn

Maynard, T., Smith, N., Gonzalez, S. (2013): Solar Storm Risk to the North American Electric Grid. Atmospheric and environmental research, Lloyd's 2013

Möstl, C., et al. (2015): Strong coronal channelling and interplanetary evolution of a solar storm up to Earth and Mars. In: Nature Communications 6, Article number: 7135 doi:10.1038/ncomms8135

NASA (2015): Solar cylce prediction. Updated 2015/08/25 http://solarscience.msfc.nasa.gov/predict.shtml

NRC (2008): Severe Space Weather Events--Understanding Societal and Economic Impacts Workshop Report, Committee on the Societal and Economic Impacts of Severe Space Weather Events: A Workshop, National Research Council, US Academy of Sciences

NSTC – National Science and Technology Council (2015): National Space Wheater Strategy. https://www.whitehouse.gov/sites/default/files/microsites/ostp/final_nationalspaceweatherstrategy_20151028.pdf

Österreichisches Studienzentrum für Frieden und Konfliktlösung – ÖSFK (2011): Stellungnahme zum Entwurf „Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten“, http://www.uni-klu.ac.at/frieden/downloads/Stellungnahme_sicherheitspolitische_Strategie_Bundesregierung.pdf

Österreichs Energie, Interessensvertretung der österreichischen E-Wirtschaft (2015): Kraftwerkskarte Österreich, Stand 27.5.2015, http://oesterreichsenergie.at/kraftwerkskarte-oesterreich.html

O'Hara, M. (2011): Why network timing accuracy is increasingly important in electronic markets. In: HFT Review – High frequency & algorithmic trading. October 31 2011. http://www.thetradingmesh.com/mod/file/download.php?file_guid=26499

Paschmann, G. (2006): Durchbruch auf ganzer Linie. In Physik Journal 5 (2006) Nr. 3., S. 16f. Übersetzte und bearbeitete Fassung eines in Nature 439, 144 (2006) erschienen Artikels. http://www.pro-physik.de/details/articlePdf/1106065/issue.html

Petermann, Thomas, Bradke, Harald, Lüllmann, Arne et al. (2011): Was bei einem Blackout geschieht – Folgen eines langandauernden und großräumigen Stromausfalls, Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag – 33, Edition Sigma Berlin, 2011

Piccinelli, R., Krausmann, E. (2014): Space Weather and Power Grids – A Vulnerability Assessment. JRC Scientific and Policy Reports, European Commission, Luxemburg 2014

Pschikal, A. (2015): Blackout: Eine kommunale Herausforderung. Vortrag bei: Österreichisches und Europäisches Programm zum Schutz kritischer Infrastrukturen (APCIP/EPCIP), Schloss Laudon, 2. September 2015

RAE - The Royal Academy of Engineering (2011): Global Navigation Space Systems: reliance and vulnerabilities. London

Reichl, J., Schmidthaler (2011): Blackouts in Österreich (BlackÖ.1). Teil I Endbericht. Energieinstitut, Johannes Kepler Universität Linz. http://www.freie-waerme.at/fileadmin/Freie-Waerme-AT/Kampagne-Sicherheitskamin/Dokumente/Studie-JKU-Blackouts-in-Oesterreich.pdf

Reichl, J., Schmidthaler, M., de Bruyn, K., Muggenhumer, G., Rebhandl, L., Frank, F., Mayr, P. et al (2015): Blackoutprävention und -intervention – Endbericht. Energieinstitut, Johannes Kepler Universität Linz. http://www.energyefficiency.at/dokumente/upload/BlackO_2_Endbericht_aa0e3.pdf

Renn, O., Dreyer, M. (2010): Vom Risikomanagement zu Risk Governance: Neue Steuerungsmodelle zur Handhabung komplexer Risiken. In: Münkler, H./Bohlender, M./Meurer, S. (Hrsg.): Handeln unter Risiko. Gestaltungsansätze zwischen Wagnis und Vorsorge. Bielefeld: transcript, 65-82

Schindler, Felix (2014): Wäre die Schweiz für ein Blackout gewappnet?, in: Online-Ausgabe des Tagesanzeigers vom 18.12.2014, http://www.tagesanzeiger.ch/schweiz/standard/Waere-die-Schweiz-fuer-ein-Blackout-gewappnet-/story/26700310

Spencer, J. (2004): The Electromagnetic Pulse Commission Warns of an Old Threat with a New Face. In: Backgrounder No. 1784, August 3 2004, the Heritage Foundation, Washington

Strobl, Theodor, Zunic, Franz (2006): Wasserbau: Aktuelle Grundlagen – Neue Entwicklungen, Springer-Verlag Berlin Heidelberg, 2006

Sturzenegger, M. (2014): Der Jahrhundertsturm könnte 2015 oder 2016 kommen. Der Tagesanzeiger, 26.07.2014. http://www.tagesanzeiger.ch/wissen/natur/Der-Jahrhundertsturm-koennte-2015-oder-2016-kommen/story/16264147

Turner, B.L., et al. (2003): A framework for vulnerability analysis in sustainability science. Proceedings of the National Academy of Sciences of the United States of America, 100 (14), 8074-8079

UK Government (2015): Space Weather Preparedness Strategy. Version 2.1, July 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/449593/BIS-15-457-space-weather-preparedness-strategy.pdf

UN/ISDR (2004): Living with Risk – A global review of disaster reduction initiatives. International strategy for disaster reduction (ISDR) Volume I, United Nations

WEF – World Economic Forum (2015): Global Risks 2015, 10th edition

Wik, M., Pirjola, R., Lundstedt, H., Viljanen, A., Wintoft, P., Pulkkinen, A. (2009): Space weather events in July 1982 and October 2003 and the effects of geomagnetically induced currents on Swedish technical systems. In: Annales Geophysicae 27, 1775-1787

Wimmer, Barbara (2015): Blackout: Österreich ist nicht ausreichend vorbereitet, futurezone 4.4.2015, http://futurezone.at/digital-life/blackout-oesterreich-ist-nicht-ausreichend-vorbereitet/123.008.911

Wolfsperger, H.A. (2008): Elektromagnetische Schirmung – Theorie und Praxisbeispiele. Springer: Berlin, Heidelberg.

Anhang

Wir danken allen Interviewpartnern und Workshopteilnehmern[7] herzlich für Ihre Kooperation und die wertvollen Inputs.

Interviews

- Atominstitut der Technischen Universität Wien
- Austrian Institute of Technology (AIT), Research Services Digital Safety & Security
- Austrian Power Grid AG (APG)
- Bundesministerium für Inneres, Abteilung für Zivilschutz und Krisenkoordination
- Bundesministerium für Landesverteidigung und Sport
- Bundesministerium für Verkehr, Innovation und Technologie, Stabsstelle für Technologietransfer und Sicherheitsforschung
- Cyber-Security Austria
- Institut für Elektrische Anlagen, Technische Universität Graz
- Institut für Hochenergiephysik, Österreichische Akademie der Wissenschaften
- Institut für Nachrichtentechnik, Technische Universität Wien
- Institut für Weltraumforschung, Österreichischen Akademie der Wissenschaften
- Zentralanstalt für Meteorologie und Geodynamik, Conrad-Observatorium

Workshop-Teilnehmer[7]

Insgesamt 12 Personen aus folgenden Organisationen:

- Bundeskanzleramt, IKT-Strategie des Bundes, Abt. I/13 E-Government Programm- und Projektmanagement
- Bundesministerium für Inneres, Sektion I, Büro für Sicherheitspolitik
- Cyber-Security Austria
- Cyber-Security Plattform der Republik Österreich
- Dipl.-Ing. Dr. Hermann Bühler GmbH
- Österreichische Akademie der Wissenschaften, Abteilung Strategie
- Österreichische Akademie der Wissenschaften, Institut für Technikfolgen-Abschätzung
- Resilienznetzwerk Österreich
- Zentralanstalt für Meteorologie und Geodynamik, Conrad-Observatorium

Abkürzungsverzeichnis

ACI ..... Austrian Critical Infrastructures
AIT..... Austrian Institute of Technology
APCIP ..... Austrian Program for Critical Infrastructure Protection
APG..... Austrian Power Grid AG
A-SIT ..... Zentrum für sichere Informationstechnologie Austria
BKA ..... Bundeskanzleramt (in dieser Studie, sonst auch: Bundeskriminalamt)
BMF..... Bundesministerium für Finanzen
BMI..... Bundesministerium für Inneres
BMLFUW..... Bundesministerium für Land- und Forstwirtschaft, Umwelt und Wasserwirtschaft
BMG ..... Bundesministerium für Gesundheit
BMLVS ..... Bundesministerium für Landesverteidigung und Sport
BMVIT ..... Bundesministerium für Verkehr, Innovation und Technologie
BMWFW..... Bundesministerium für Wissenschaft, Forschung und Wirtschaft
BSI ..... Bundesamt für Sicherheit in der Informationstechnologie (Deutschland)
bspw. ..... beispielsweise
bzw. ..... beziehungsweise
CERT ..... Computer Emergency Response Team
CIP ..... Critical Infrastructure Protection
CME ..... Coronal Mass Ejection, Koronaler Massenauswurf
d. h. ..... das heißt
DC ..... Defence Committee, in dem Fall: des brit. House of Commons
etc. ..... et cetera, wörtlich: und die übrigen, in der Bedeutung von: und so weiter
EKC..... Einsatz- und Krisenkoordinationscenter des BMI
EKI ..... Europäische kritische Infrastrukturen
EMP..... Elektromagnetischer (Im)Puls
EMV..... Elektromagnetische Verträglichkeit
ENTSO-E..... European Network of Transmission System Operators for Electricity, Verband europäischer Übertragungsnetzbetreiber
ESA ..... European Space Agency
EU..... Europäische Union
FFG ..... Forschungsförderungsgesellschaft
ggfs. ..... gegebenenfalls
GHz ..... Gigahertz
GIC ..... geomagnetically induced currents
GMD ..... geomagnetic disturbances
GPS ..... Global Positioning System
GWh ..... Gigawattstunden
HEMP ..... High altitude (nuclear) EMP
HPM..... High Power Microwave
Hz ..... Hertz
i.d.R. ..... in der Regel
IKT..... Informations- und Kommunikationstechnologie
IKTS..... IKT-Strategie des Bundes
ISDR ..... Internationale Strategie zur Reduzierung von Katastrophen, International Strategy for Desaster Reduction
IT ..... Informationstechnologie
ITA..... Institut für Technikfolgen-Abschätzung an der ÖAW
IWF ..... Institu für Weltraumforschung an der ÖAW
HFT..... High Frequency Trading
KI ..... Kritische Infrastruktur(en)
KKM..... Krisen- und Katastrophenschutzmanagement
km..... Kilometer
km/h..... Kilometer pro Stunde
km/s ..... Kilometer pro Sekunde
KSÖ ..... Kuratorium Sicheres Österreich

kV ..... Kilovolt
LEMP ..... Lightning electromagnetic pulse
lt. ..... laut
M2M ..... machine to machine
MeV ..... Megaelektronenvolt
MHz ..... Megahertz
MW ..... Megawatt
NASA ..... National Aeronautics and Space Administration (USA)
NEMP ..... Nuclear EMP
NEP ..... Netzausbauplan
NY ..... New York
o.dgl. ..... oder dergleichen
ÖAW ..... Österreichische Akademie der Wissenschaften
ÖSCS ..... Österreichische Strategie für Cyber-Sicherheit
ÖSFK ..... Österreichisches Studienzentrum für Frieden und Konfliktlösung
ÖSS ..... Österreichische Sicherheitsstrategie
PDÖ ..... Plattform Digitales Österreich
RG CE ..... Regional Group Central Europe
RTR ..... Rundfunk und Telekom Regulierungs-GmbH
SCADA ..... Supervisory Control and Data Acquisition
SKKM ..... Staatliches Krisen- und Katastrophenschutzmanagement
sog. ..... so genannte
TETRA ..... terrestrial trunked radio, urspr. trans-european trunked radio
TAB ..... Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag
u. a. ..... unter anderen/anderem
UK ..... United Kingdom, Vereinigtes Königreich Großbritannien und Nordirland
UN ..... United Nations, Vereinte Nationen
urspr. ..... ursprünglich
USA ..... United States of America, Vereinigte Staaten von Amerika
UVP ..... Umweltverträglichkeitsprüfung
UWB ..... Ultra Wide Band
vgl. ..... vergleiche
VIX ..... Vienna Internet Exchange
ZAMG ..... Zentralanstalt für Meteorologie und Geodynamik
z. B. ..... zum Beispiel

Glossar

Cyber-War ..... Ist eine kriegerische Auseinandersetzung im virtuellen Raum, meistens über Kommunikationsnetze ausgetragen. Bezeichnet bisweilen auch moderne, hochtechnisierte Kriegsführung, bei der alle Mittel der Kriegsführung miteinander vernetzt sind.

Denial of Service, DoS .... Angriff auf einen Server über das Netzwerk/Internet, bei dem der Server mit (beschädigten) Datenpaketen geflutet wird, die er nicht schnell genug verarbeiten kann, wodurch das Antwortverhalten so schlecht wird, das reguläre Verbindungen zu lange warten müssen und abbrechen.

endogen ..... Aus dem Inneren eines Systems

Exposition ..... Hier: Die Summe aller (schädigenden) Umwelteinflüsse, denen ein System ausgesetzt ist.

exogen ..... Von außen auf ein System einwirkend

Forecasting	Eine Methode Prognosen für die Zukunft zu erstellen, die auf Daten aus der Vergangenheit und Trendanalysen beruht.
Foresight	Vorausschau, Blick in die Zukunft, die Fähigkeit den Weg in eine gewünschte Zukunft definieren zu können.
High Frequency Trading	(Hochfrequenzhandel) Bezeichnet den Computer-basierten Handel mit Wertpapieren, der sich durch extrem kurze Haltefristen auszeichnet; von Menschen in der Geschwindigkeit nicht mehr durchführbar.
Induktion	Bezeichnet die Entstehung eines elektrischen Feldes durch eine Änderung der magnetischen Flussdichte.
Industrie 4.0	Verzahnung der industriellen Produktion mit Informations- und Kommunikationstechnologie.
Internet der Dinge	Das Internet der Dinge bezeichnet eine Vielzahl miteinander vernetzter Alltagsgegenstände.
Kondensator	Ist ein elektrisches Bauelement, das in der Lage ist elektrische Ladungen bzw. Energie aufbauend zu speichern, und die gesamte gespeicherte Ladung auf einmal abzugeben.
Meta-System	Ein übergeordnetes System, dessen Systemkomponenten aus anderen Systemen bestehen.
Notstromaggregat	Liefert bei einem Stromausfall elektrische Energie aus einer Batterie und/oder einem Verbrennungsmotor
Peak	Höhepunkt
Photon	Ein Photon ist das Elementarteilchen eines elektromagnetischen Feldes, das woraus elektromagnetische Strahlung „besteht“.
Redundanz	Hier: Das zusätzliche Vorhandensein (funktions-)gleicher Komponenten oder Systeme, die im Normalbetrieb nicht nötig wären, aber so implementiert sind, dass sie bei Ausfall einer anderen Komponente deren Funktion im System übernehmen können.
Resilienz	Die Fähigkeit eines Systems nach einem Systemschock in den Ausgangszustand zurückzufinden.
Schnittstelle	Teil eines Systems, das der Kommunikation mit anderen Systemen dient, und diese damit verbindet.
Sektor	Hier: Branche
Transdisziplinarität	als Prinzip sog. integrativer Forschung berücksichtigt Transdisziplinarität methodisch nicht nur wissenschaftlich gesichertes sondern auch praktisches Wissen. Das ist besonders dort nützlich, wo das Wissen zu einem bestimmten Problem unsicher ist, vielleicht auch das Problem noch nicht ganz klar ist, und dort, wo es darum geht implizit vorhandenes Wissen explizit zu machen.
Transformator/Trafo	Elektrotechnisches Bauelement zur Spannungswandlung.
Umspannwerk	Ein Umspannwerk ist Teil eines elektrischen Versorgungsnetzes und verbindet Netze mit unterschiedlichen Spannungsebenen.
Vulnerabilität	Verwundbarkeit, Angreifbarkeit von Systemen oder Infrastruktur-Komponenten