# Resilienz digitaler Energiesysteme

## Oder: Warum Resilienzstrategien im Zeitalter der Digitalisierung überlebenswichtig sind

9. Nordhessisches Energiegespräch, SUN
12.9.2019, Kassel

Prof. Dr. Bernd Hirschl
IÖW – Institut für ökologische Wirtschaftsforschung, Berlin
und
BTU Cottbus-Senftenberg

# Kurzvorstellung
# Prof. Dr. phil. Dipl-Ing-Oec. Bernd Hirschl

- **Leiter der Abteilung Nachhaltige Energiewirtschaft und Klimaschutz am Institut für ökologische Wirtschaftsforschung IÖW (GmbH, gemeinnützig), Berlin**

  i | ö | w

  - seit 1985 Forschung und Politikberatung für nachhaltiges Wirtschaften
  - Standorte Berlin und Heidelberg, über 60 Mitarbeiter/innen aus Wirtschafts- und Sozial-, Ingenieur- und Naturwissenschaften
  - Langjährige Erfahrungen in der Analyse, Entwicklung und Bewertung von Innovationen und Märkten sowie politischen Instrumenten und Klimaschutzstrategien
  - Unabhängig, 100% durch Drittmittel finanziert; überwiegend öffentliche Auftraggeber
  - www.ioew.de

- **Leiter Fachgebiet Management regionaler Energieversorgungssysteme an der Brandenburgischen Technischen Universität (BTU) Cottbus-Senftenberg (Lausitz)**

  b-tu

  - https://www.b-tu.de/fg-energieversorgungsstrukturen

- **Ausgewählte Funktionen**
  - Mitarbeit im Akademienprojekt Energiesysteme der Zukunft ESYS, u.a. AG Resilienz digitaler Energiesysteme, AG De/Zentrales Energiesystem
  - Sprecher des Berliner Klimaschutzrates

# Inhalt

- **Megatrends Digitalisierung und Elektrifizierung**
- **Das blackout-Risiko**
- **Das Konzept der Resilienz**
- **Der zellulare Ansatz**
  - Konzept / Kosten-Nutzen / Umsetzung
- **Fazit**

*Hinweis: in dieser Fassung wurden die gezeigten Bilder aus urheberrechtl. Gründen entfernt*

# Megatrends Digitalisierung und Elektrifizierung
## Oder: Das digitale Stromsystem wird zur Leit-Infrastruktur

- **Einst unabhängige, jetzt eng gekoppelte Megatrends**
  - Digitalisierung findet (seit Jahren) in allen Sektoren statt – auch im Stromsystem
  - Elektrifizierung findet (seit Jahrzehnten) in allen Sektoren/ Infrastrukturen statt
  - Stromwende/ Energiewende braucht verstärkt Digitalisierung (enabling technology) für effiziente Koordination einer Vielzahl von Akteuren, Anlagen und Prozessen (am besten in Echtzeit)
  - Digitalisierung braucht (zunehmend viel) Strom
- **Strom und IKT prägen ALLE anderen Infrastrukturen – auch alle kritischen Infrastrukturen (KRITIS)**
- **Beide Megatrends weisen enorme (ökonomische) Chancen auf – aber auch hohe (gesellschaftliche) Risiken**

# Das größte Risiko: ein langanhaltender, großflächiger Blackout

- **„gewöhnliche“ Blackoutgefahren bzw. Ursachen**
  - Lokale Infrastrukturschäden und Hardware-Störungen (durch z.B. Extremwetter, Terroranschläge o.ä.)
    - idR durch N-1 geschützt, Schadensgebiet regional begrenzt, Reparatur möglich
- **Stressoren für die Stabilität des Stromnetzes**
  - Schwankungen durch Erneuerbare Energien (Erzeugung) …
  - … und/oder durch Marknachfrage bzw. Marktdesign (insb. Strombörse, aber auch Regelenergiemärkte, perspektivisch Gleichzeitigkeitseffekte beim Laden von E-Mobilität)
  - Beides idR durch die Marktakteure/ Netzbetreiber gut beherrschbar (verbesserte Prognosegüte, Ausbau Netzkapazität und SDL etc.)
- **Digitalisierung bringt (insbes. durch Hackerangriffe) eine neue Qualität der Verwundbarkeit mit sich, die alle anderen Stressoren deutlich übersteigt**

Quelle: Projekt „Strom-Resilienz“ von IÖW / Uni Bremen

# Beispiele von Cyberattacken auf Energieinfrastrukturen (weltweit)

| Year | Target | Name of the attack | Consequences | Objective | Attackers |
|---|---|---|---|---|---|
| **1982** | **Explosion of a gas pipeline in Siberia (Russia)** | | **Malware introduced into the SCADA managing the pipeline, the explosion was equivalent to 3 tonnes of TNT.** | **Sabotage** | **External** |
| 1992 | warning system at Chevron, (USA) | | discovered when an accident took place at the Chevron refinery in Richmond, during which thousands of people living nearby were exposed to toxic substances for about 10 hours. | Sabotage | Internal |
| 1999 | Gazprom, (Russia) | | Takeover of the distribution panel controlling gas flows through pipelines. | Sabotage | Internal |
| 1999 | Gas pipeline in Bellingham (USA) | | This accident was linked to the development of a database for the SCADA system operating the pipelines of the Olympic Pipe Line company. The accident was partly responsible for the spillage of oil causing three deaths and several injuries. | Accident/ human error | Internal |
| 2001 | Electricity operator California, (USA) | | The attackers had access to one of the internal networks of the California Independent System operator. The attack only affected the PLC network of the company before being discovered. | Sabotage | External/ China? |
| 2003 | Davis-Besse Nuclear-power, | Slammer | Shutdown of the parameter display system for four hours due to a worm, with no espionage or sabotage | Not targeted | External |
| **2010** | **Natanz, (Iran)** | **Stuxnet** | **Several years of infiltrating the uranium enrichment at Natanz, damaging more than 900 uranium enrichment centrifuges.** | **Sabotage** | **External/ State-sponsored/ USA, Israel?** |
| 2011 | Energy industries | Duqu | Parts of code nearly identical to Stuxnet, designed only for industrial espionage, without any destructive function. | Espionage | External |
| 2011 | Areva, (France) | | Theft of non-critical company data. Infiltration over two years. | Espionage | External |
| 2012 | Companies and institutions linked to energy | Flame | Widespread in the Middle East and North Africa, operated for at least two years. Designed for espionage and data analysis. Discovered after Iran's Ministry of Oil and the Iranian National Oil Company had reported theft and the erasure of some important data from their systems. | Espionage/ data theft | External |
| 2012 | Saudi Aramco, (Saudi Arabia) | Shamoon | 30,000 hard disks destroyed and to be replaced, no impact on the operational network. | Sabotage | External |
| 2013 | Bowman Avenue Dam, (USA) | | Attackers had taken remote control of a small dam near New York, with no consequences. | Reconnaissance | External/ Iran? |
| **2015** | **Electricity operators, (Ukraine)** | **Black Energy** | **30 electricity substations disconnected from the grid, eight provinces without electricity for several hours, more than 200,000 people affected, ICS physically damaged, substations manually operated for several weeks after the event.** | **Sabotage** | **External/ State-sponsored, Russia?** |

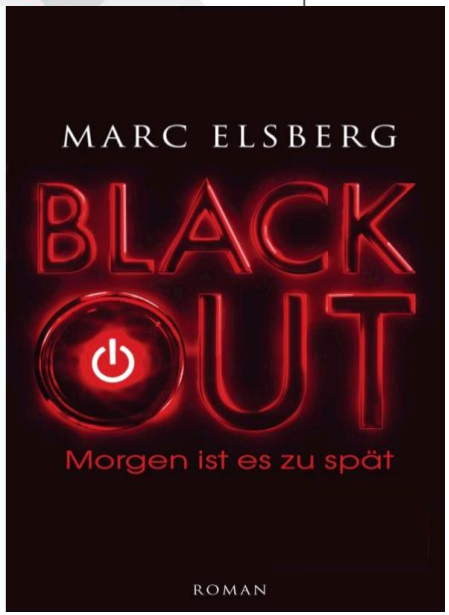
**„Cyber-Abwehrzentrum warnt nach Hacker-Angriffen auf das ukrainische Stromnetz vor Stromausfall in ganz Europa“ (Der Spiegel, 24.08.2018)**

**Geschätzte Schäden von Cyber-Crime weltweit (2017): 500-600 Mrd. Dollar**

Quelle: Gabrielle Desarnaud (2017): Cyber Attacks and Energy Infrastructures: Anticipating Risks, Études de l'Ifri (Institut français des relations internationales), S. 19-20

# Das größte Risiko: ein langanhaltender, großflächiger Blackout

- **Ein langanhaltender großflächiger Blackout betrifft ALLE anderen Infrastrukturen & KRITIS, für die es nach heutigem Stand nur unzureichende Notversorgungslösungen gibt**
  - Z.B. Krankenhäuser, Trink- und Abwasserversorgung, Nahrungsmittelversorgung, Gewährung von Sicherheit und Schutz wichtiger Einrichtungen und der Bevölkerung etc.
- **Ein langanhaltender großflächiger blackout stellt damit eine gravierende Gefahr für den gesellschaftlichen Zusammenhalt – für die menschliche Zivilisation an sich dar - und ist daher zwingend zu vermeiden**
- **Zwischenfazit**
  - Digitale Energiesysteme sind inhärent verwundbar - und können nicht vollständig geschützt werden
  - Zentrale und dezentrale – digitale - Energiesysteme sind gleichermaßen verwundbar
    - Gründe: zentrale Elemente auch in dezentralen Systemen, human factor etc.
  - ➢ Vor diesem Hintergrund sollte die Erhöhung der Resilienz digitaler Energiesysteme höchste Priorität haben


Quelle: Projekt „Strom-Resilienz“ von IÖW / Uni Bremen

# Das Konzept der Resilienz für ein digitales Energiesystem

- **Resilienz ist im allg. definierbar als**
  - „die Fähigkeit eines Systems, seine Funktionsfähigkeit unter Belastungen aufrechtzuerhalten beziehungsweise kurzfristig wiederherzustellen“ (ESYS 2017)
- **Notwendig (aber nicht hinreichend): IT-Sicherheit (Prävention)**
  - Akteure: staatliche Behörden, Wirtschaft, Bürger
  - Grundbedingungen: Datenschutz und -sicherheit, Datensouveränität und –sparsamkeit
  - Erforderlich: aktuelle und wirksame Schutzsoftware - und Nutzer, die sie einsetzen (Bildung / Aufklärung), IT-OT-Trennung, …
- **Für den Fall eines großflächigen Blackouts durch Hackerangriffe ist jedoch der Fall zu befürchten, dass eine kurzfristige Wiederherstellung des (heutigen) Gesamtsystems nicht möglich ist**

➢ **im Krisenfall ist eine lokale/ regionale (Mindest-)Versorgung unabhängig vom übergeordneten Netz zu gewährleisten!**

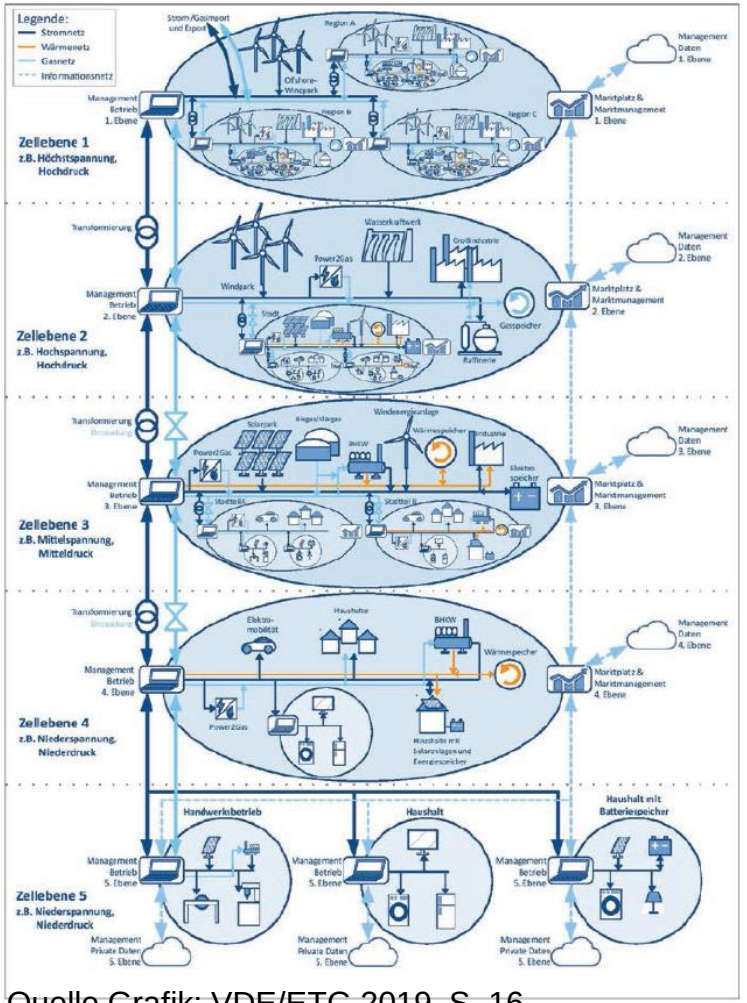
# Ein resilientes digitales Energiesystem – der zellulare Ansatz

- **Gegenwärtiges Energiesystem: überregionale Infrastrukturen und Marktanreize (z.B. Strombörse, Regelenergiemärkte)**
  - In einem zentralen, überregionalen Energiesystem kann ein „Single Point of Failure“ (inkl. Dominoeffekt) kritische Situationen bis hin zu blackouts auslösen


- **Ein (vernetzt) zellulares Energiesystem verringert die Verwundbarkeit**
  - Defintion für den Normalbetrieb: „Im **zellular geprägten Energiesystem** wird nach dem **Subsidiaritätsprinzip** die physikalische Balance zwischen Energieangebot und -nachfrage soweit wie möglich bereits auf regionaler, lokaler Ebene hergestellt.“ (VDE/ETG 2019)
  - Durch Nutzung von **Flexibilität und Sektorenkopplung** vor Ort kann auch der **Ausbaubedarf im Verteil- und Übertragungsnetz** sowie die **Anzahl von Stabilisierungsmaßnahmen gemindert** werden

# Ein resilientes digitales Energiesystem – der zellulare Ansatz

- **Arten von (neben- und ineinander geschachtelten) Zellen**
  - Gebäude, Betriebe, Objekte als „Prosumer“ (Erzeuger&Verbraucher)
  - Blöcke, Quartiere, Stadtteile als „gemeinschaftliche Eigenverbraucher“
  - Regionalstromanbieter im Verteilnetz
  - …
- **Im Krisenfall: Zelle funktioniert als inselnetzfähiges bzw. autarkiefähiges Teilsystem**
  - Mindesterzeugung mit erneuerbaren Energien in jeder Zelle, um zumindest KRITIS zu versorgen
  - dafür Rekonfiguration der Verteilnetzstruktur in Stadt-Umlandnetze sinnvoll
  - Idealerweise Offline-Betrieb möglich, sonst IKT-Backup je Zelle
  - Bottom-up Wiederaufbaufähigkeit




Quelle Grafik: VDE/ETG 2019, S. 16

# Der zellulare Ansatz
# Abwägungen zu Kosten und Nutzen

- **Kosten für Resilienz spielen in heutigen Modellen nur untergeordnete Rolle – ebenso wenig die möglichen Schäden eines langanhaltenden, großflächigen Blackouts**
- **Die heutige Debatte und die Wahl der politischen Instrumente sind zwar geprägt von (spezifischer) Kosteneffizienz – aber nicht von Systemeffizienz**
  - Z.B. Strombörsenpreissignal und verpflichtende Direktvermarktung vs. Verteilnetzengpass, EEG-Ausschreibungen vs. systemisch sinnvolle Standorte, …
- **In einer idealen Welt der sog. Kupferplatte (vollständig ausgebautes Netz) sind (dezentral verteilte) zellulare Lösungen tendenziell teurer**
  - Ideale (europäische) Kupferplatte voraussichtlich auf absehbare Zeit nicht erreichbar
- **aber: ein regional verteilter Ausbau erneuerbarer Energien erscheint ohnehin dringend erforderlich angesichts von Netzausbauproblemen, steigender Kosten für Systemdienstleistungen und Abregelung und zur Erreichung der Klimaschutzziele**
- **Nutzenaspekte / Co-Benefits zellularer Strukturen**
  - regionale Verteilung von Erzeugung und Flexibilität erzeugt Wertschöpfung vor Ort, stärkt die Akzeptanz und die Erschließung der knappen Flächen

# Der zellulare Ansatz
# mögliche Maßnahmen für den Übergang

- **Der bestehende rechtliche Rahmen begünstigt heute**
  - weder eine regionale Verteilung von Erzeugung / die Bereitstellung von Flexibilität und Speichern (weder regional noch überregional)
  - noch die Bildung von Zellen
- **Mögliche Maßnahmen zur Stärkung/ Bildung zellularer Strukturen (Auswahl)**
  - Erzeugung
    - Vorgabe je Region: 2% EE-Anteil der  Fläche / Stärkung kommunaler Entscheidungen, Bürgerenergie und Stadtwerke / Anwendung De Minimis bei Ausschreibungen gemäß EU-Recht
    - Stärkung von (netzdienlichem!) Eigenverbrauch (Prosuming), auch gemeinschaftlichen Eigenverbrauch, Mieterstrom / ambitionierte Umsetzung neuer EU-Richtlinie!
  - Marktregeln regionalisieren
    - Stärkung Regionalstrom, Quartierslösungen, Flexibilität, Plattformen, Bilanzkreisverantwortung – jeweils im Verteilnetz
  - Stärkung Systemverantwortung für Verteilnetzbetreiber und EVU
    - Ambitionierte Umsetzung neuer EU-Regeln (Grid Codes)
    - Rekonfiguration Verteilnetzstrukturen (Stadt-Umland)
  - …

# Fazit

- Die **Digitalisierung** bietet viele Chance und Potenziale – birgt jedoch auch die große Gefahr eines **langanhaltenden, großflächigen Blackouts**
- Das **digitale Stromsystem** ist bereits heute die zentrale **Leit-Infrastruktur** – und die Bedeutung wird weiter zunehmen (Sektorkopplung)
- Damit muss die Erhöhung der **Resilienz des digitalen Energiesystems** in den Vordergrund rücken – in der Wissenschaft (Technik, Ökonomie, Gesellschaftswissenschaften), Praxis und Politik
- **Zellulare Strukturen** können die Verwundbarkeit, den Netzausbau- und Abregelungsbedarf mindern und die Resilienz und Versorgungssicherheit erhöhen
- Der derzeitige **politische Rahmen** ermöglicht keine Transformation in Richtung eines zellularen Systems
- Der bestehende Rahmen kann **schrittweise reformiert** werden – dies ist jedoch bereits bei den anstehenden Debatten um $CO_2$-Bepreisung und EEG-Reformen zwingend mit zu berücksichtigen - aktuelle EU-Regeln unterstützen hierbei
- Zellulare Strukturen können viele „**Co-Benefits**“ aufweisen, die kritisch für den weiteren Erfolg der Energiewende sind: verteilte Erzeugung und damit effiziente Nutzung der knappen Flächen, Erhöhung der Akzeptanz, Schaffung regionaler Wertschöpfung und Beschäftigung durch die Energiewende

# Vielen Dank.

Prof. Dr. Bernd Hirschl
IÖW – Institut für ökologische Wirtschaftsforschung, Berlin
und
BTU Cottbus-Senftenberg

12.9.2019