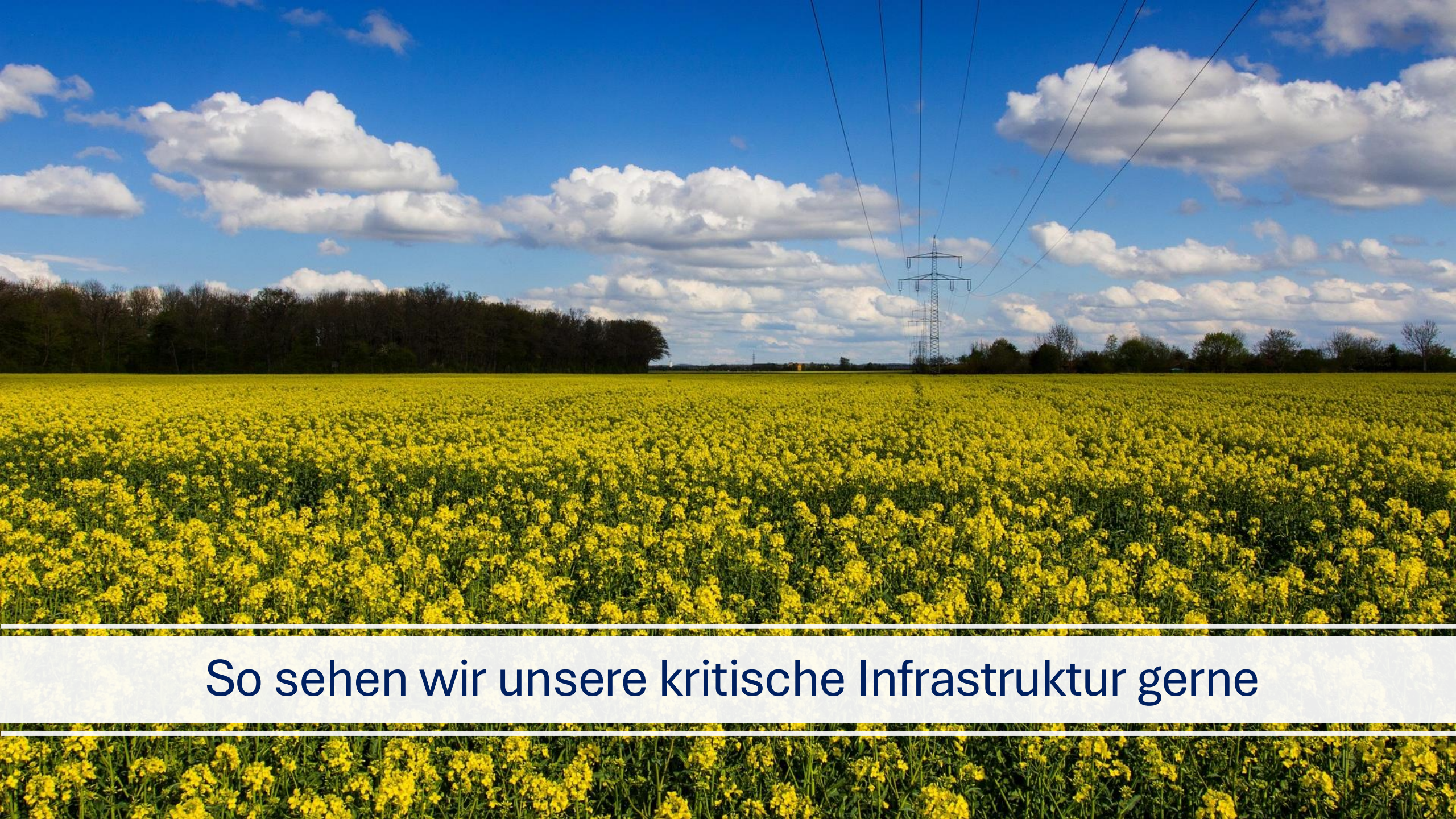
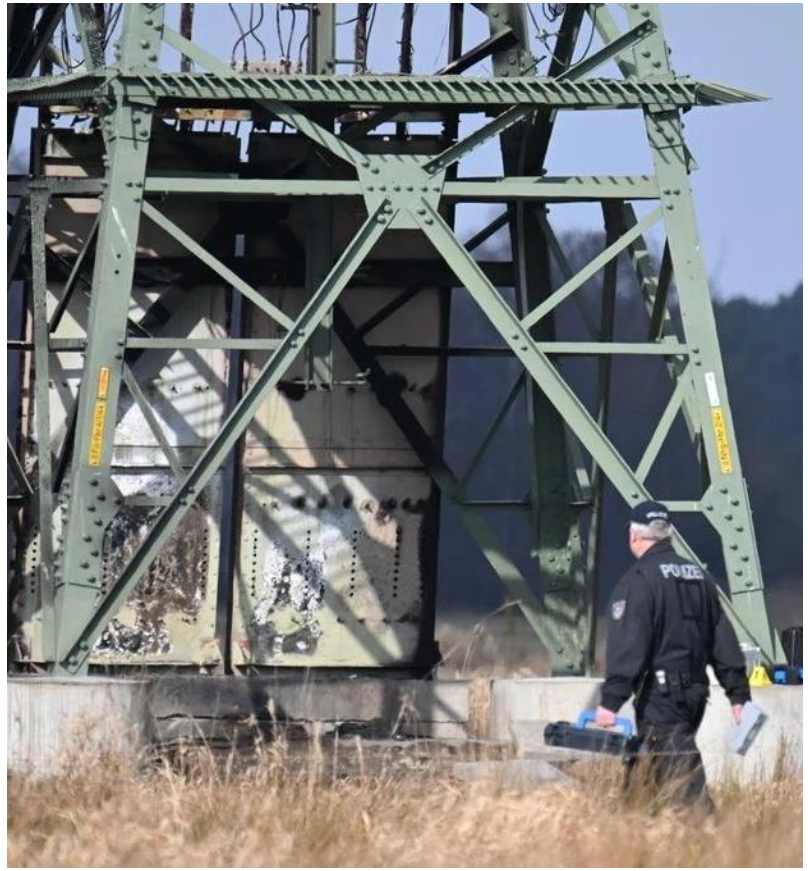
Stärkung der Resilienz im Netzbetrieb in einer hybriden Gefahrenlage

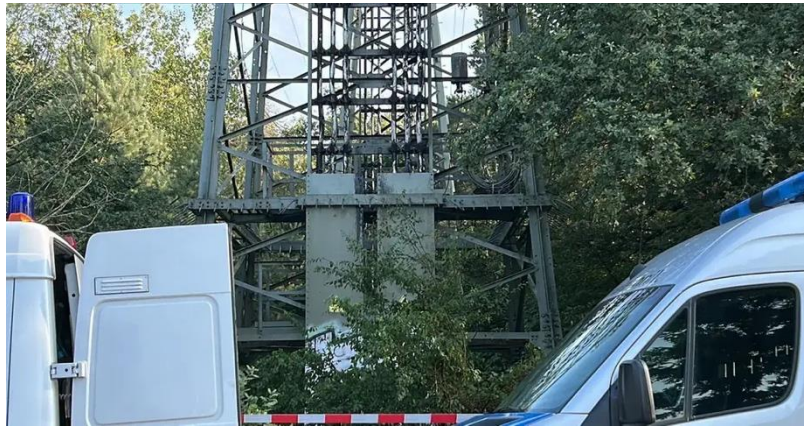
Impuls zum ESYS-Deepdive am 9. Februar 2026

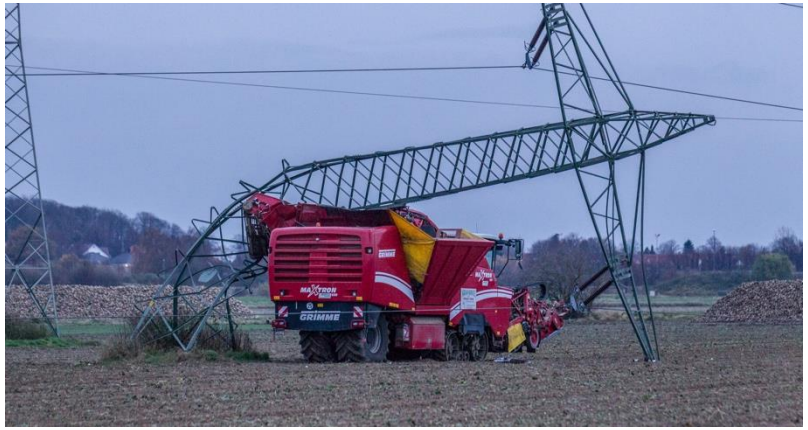
Dr. Stefan Küppers, ehem. CTO Westenergie AG

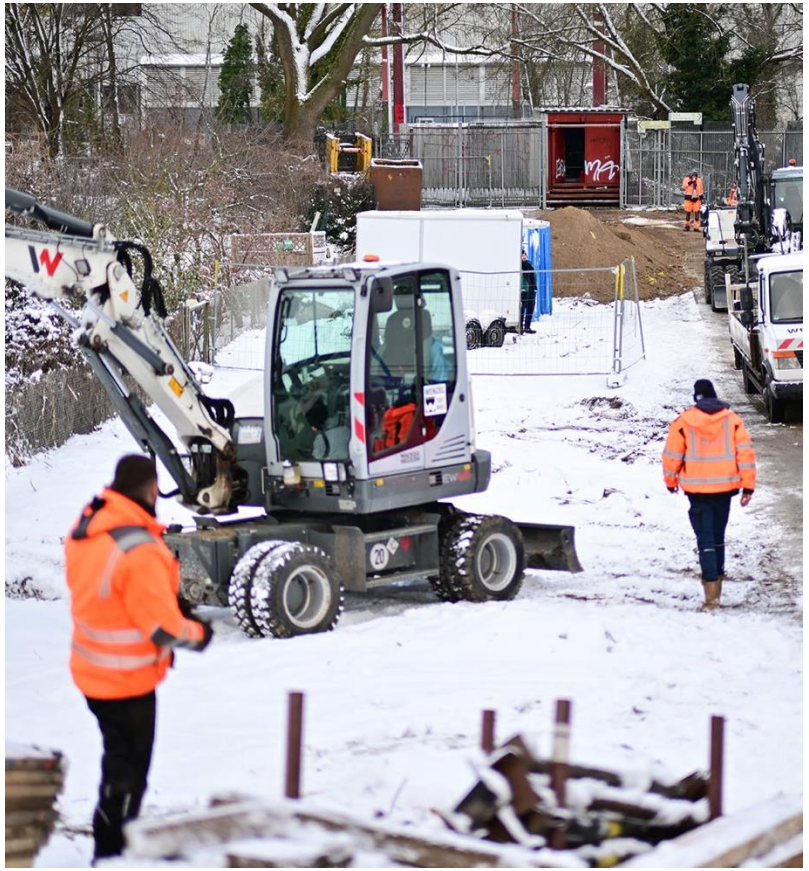


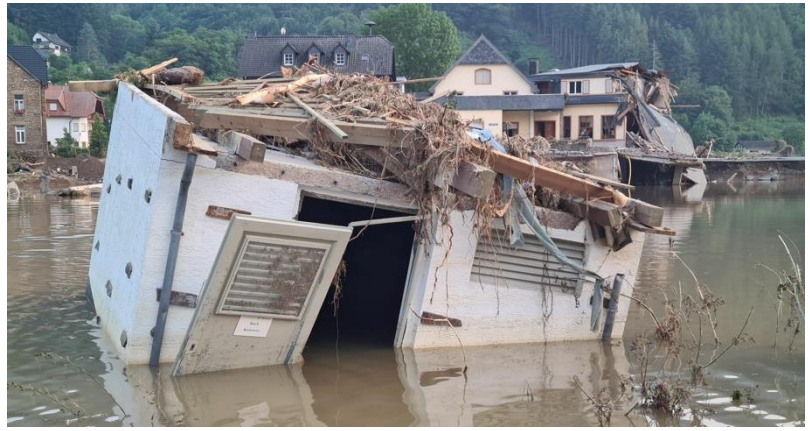
So sehen wir unsere kritische Infrastruktur gerne





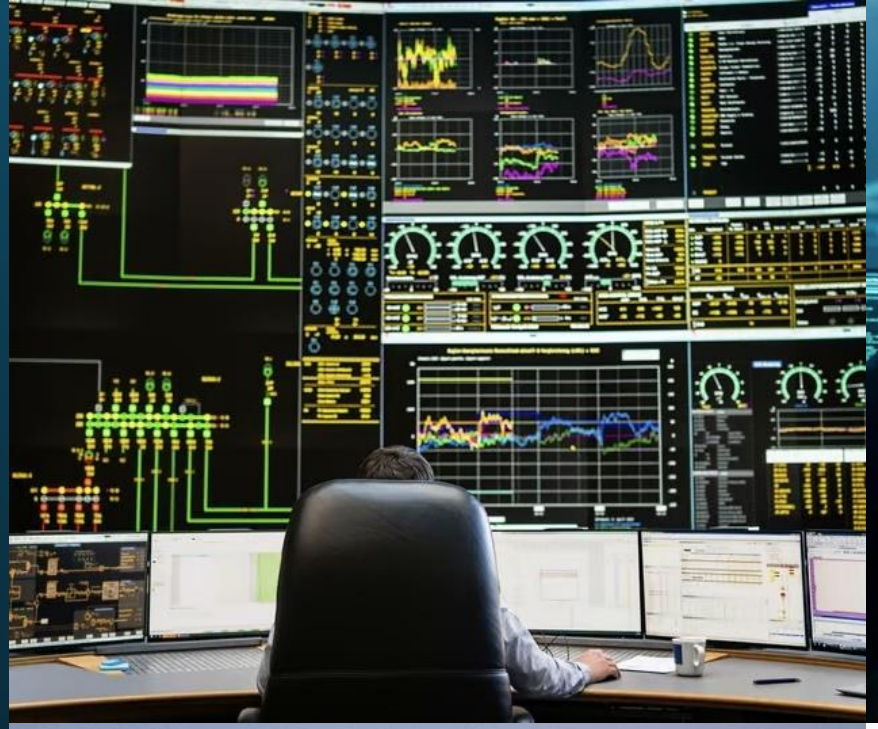


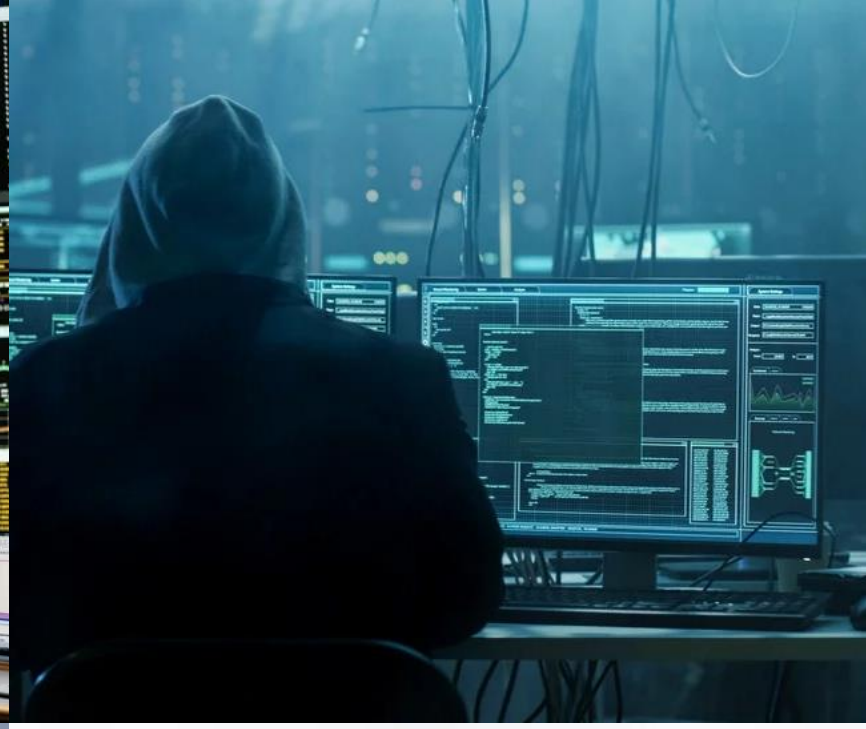


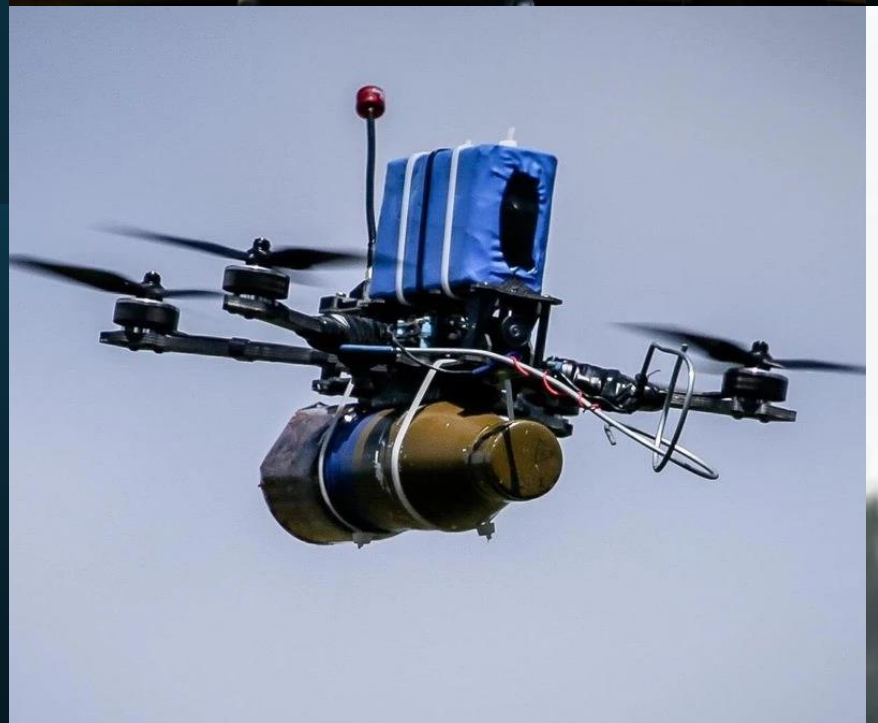


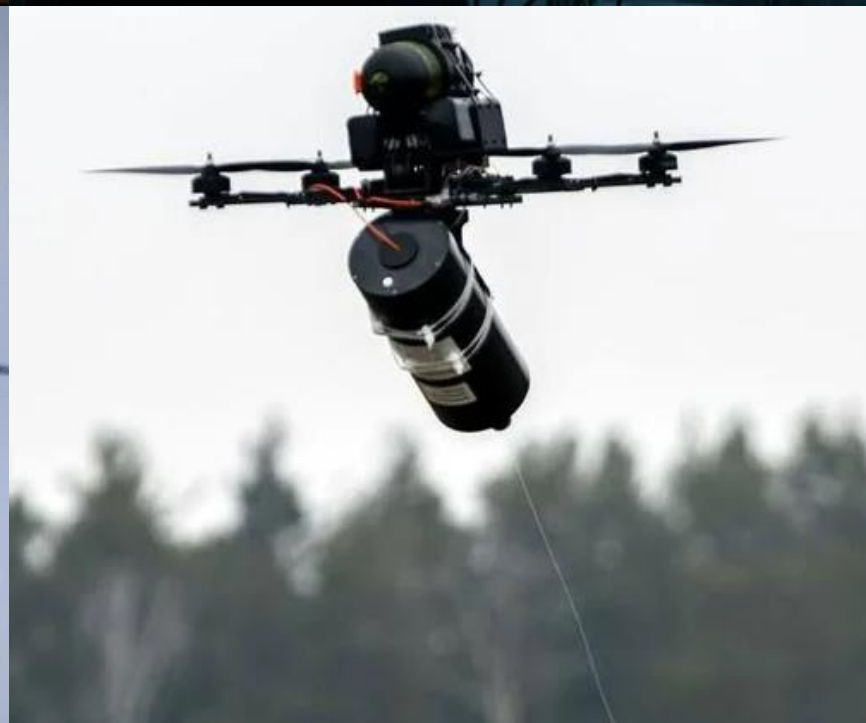
Vielfältige physische Einflussfaktoren können aber zu Störungen und Stromausfällen führen

Cyberangriffe gibt es schon lange und Drohnenattacken sind wahrschein-licher geworden









Was ist eigentlich Resilienz in der Energieversorgung?

- **Resilienz** bezeichnet die Fähigkeit eines Systems, **Ereignissen** zu widerstehen oder sich daran anzupassen und dabei seine Funktionsfähigkeit zu erhalten oder schnell wiederzuerlangen.*
- **Ereignisse** können z.B. Naturereignisse, physische Angriffe, Cyber-Angriffe oder Verlust der Systemstabilität sein.

*Quelle: BMI

Ein Phasenmodell zur Verbesserung der Resilienz

1. Analyse aller Risiken und Planung geeigneter Maßnahmen
2. Aufbau des Schutzes kritischer Komponenten und Sicherung „erfolgskritischer“ Ressourcen
3. Überwachung der Infrastruktur, Erfassung kritischer Ereignisse und kontinuierliche Bewertung der Lage
4. Reaktion auf Ereignisse und Störungen bzw. Unterbrechungen
5. Wiederherstellung des Systems

Dabei: Kontinuierliche Verbesserung und Entwicklung der Prozesse

Die Verbesserung der Resilienz ist im Gange

- Spätestens seit Beginn des Kriegs in der Ukraine ist klar, dass die kritische Infrastruktur ein bevorzugtes Angriffsziel ist.
- Viele Ansätze sind implementiert, um den Schutz zu erhöhen.
- Das KRITIS-Dachgesetz und die NIS-Richtlinie sind zwei weitere Regelwerke, das Schutzniveau zu erhöhen.
- BDEW („10-Punkte-Papier“) und VDE-FNN (Hinweis „Aufbau und Betrieb resilienter Stromnetzinfrastrukturen“) haben Papiere dazu veröffentlicht.
- Die Unternehmen müssen – falls noch nicht begonnen - ihre Ansätze und Regeln überprüfen sowie kritische Ressourcen und Materialien ergänzen.
- Alle Beteiligte müssen viel mehr und regelmäßig üben.
- Gegenseitige Unterstützung der Netzbetreiber ist langjährig geübte Praxis.
- **Aber: Einen vollständigen Schutz und eine absolute Sicherheit vor Zerstörung von Anlagen und Komponenten gibt es nicht!**

Einige Knackpunkte und Grenzen

- Die Verbesserung der Resilienz in der kritischen Infrastruktur erfordert eine **Integration aller Sicherheits-Management-Systeme** (ISMS, PSIM, BCM etc.)
- Eine **klare Struktur** und Organisation des **Krisenmanagements** im föderalen System Deutschland ist erforderlich
- Die Herstellung einer höheren Resilienz erfordert **zusätzliche Finanzmittel**
  - Kontinuierlicher Druck zur Senkung die Betriebskosten durch die Regulierung ist kontraproduktiv
  - Run auf Netzanschlüsse für Batteriespeicher und Rechenzentren sowie die der Anschluss der EE-Anlagen binden die Investitionsmittel und notwendige Ressourcen
- Es braucht eine **gesicherte Kommunikationstechnik** für die kritische Infrastruktur (z.B. 450 MHz Funknetz)
- Allerdings müssen sich auch **Kunden** gemäß NAV besser auf Notfälle einstellen

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Stefan Küppers
Email: dr.stefan.kueppers@web.de