

A black and white photograph of an industrial facility, likely a refinery or chemical plant. The image shows a complex network of large pipes, metal structures, and scaffolding. In the foreground, a large, dark, curved pipe dominates the left side. In the background, a tall, multi-story industrial tower is visible. The overall scene is industrial and technical.

Swisscom Security Conference 2022

Manuel „HonkHase“ Atug



Die KRITISche Bedrohungslage

Manuel ‚HonkHase‘ Atug

Ich habe #KRITIS im Endstadium

Manuel (HonkHase) Atug

Head of Business Development bei der HiSolutions AG

- Dipl.-Informatiker, Master in Applied IT Security, Ingenieur
- Weit über 23 Jahren in der Informationssicherheit tätig
- Sachverständiger für das IT-SiG 2.0 im Bundestag
- Themen: KRITIS, Hackback, Ethik, Hybrid Warfare, Cyberresilienz, Bevölkerungs- und Katastrophenschutz

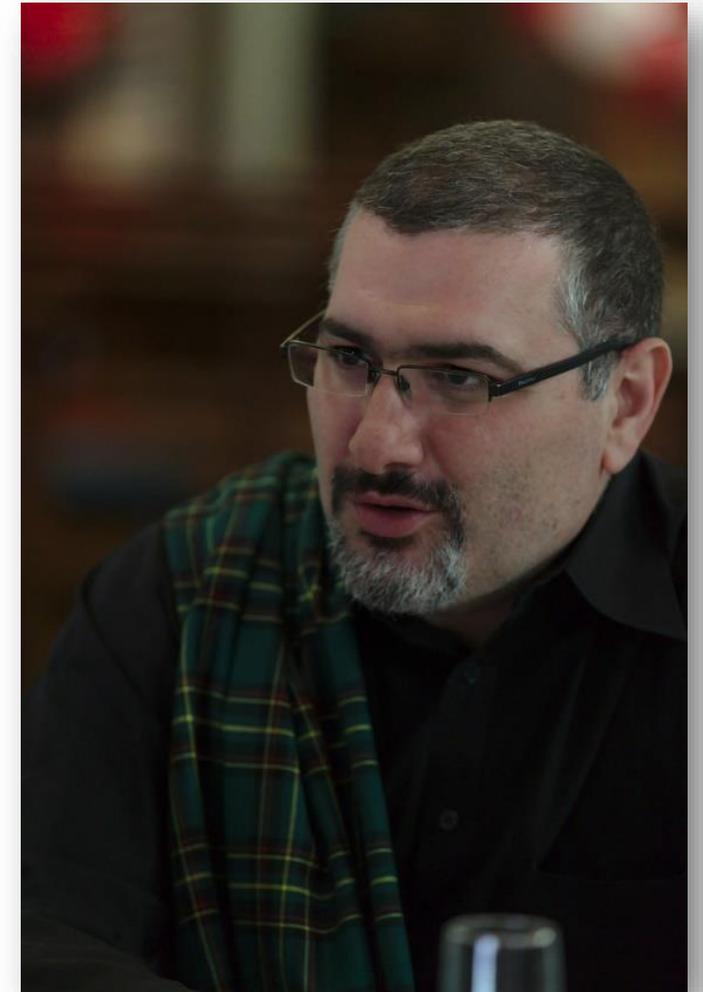
- Mitgründer der AG KRITIS: ag.kritis.info



- Mitgründer der AGND: www.agnd.eu



 [@HonkHase](https://twitter.com/HonkHase)  [@HonkHase@chaos.social](https://chaos.social/@HonkHase)



Was sind KRITISche Infrastrukturen?



10 Kritische Infrastruktur Sektoren in Deutschland



Quelle https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sectoren-branchen_node.html



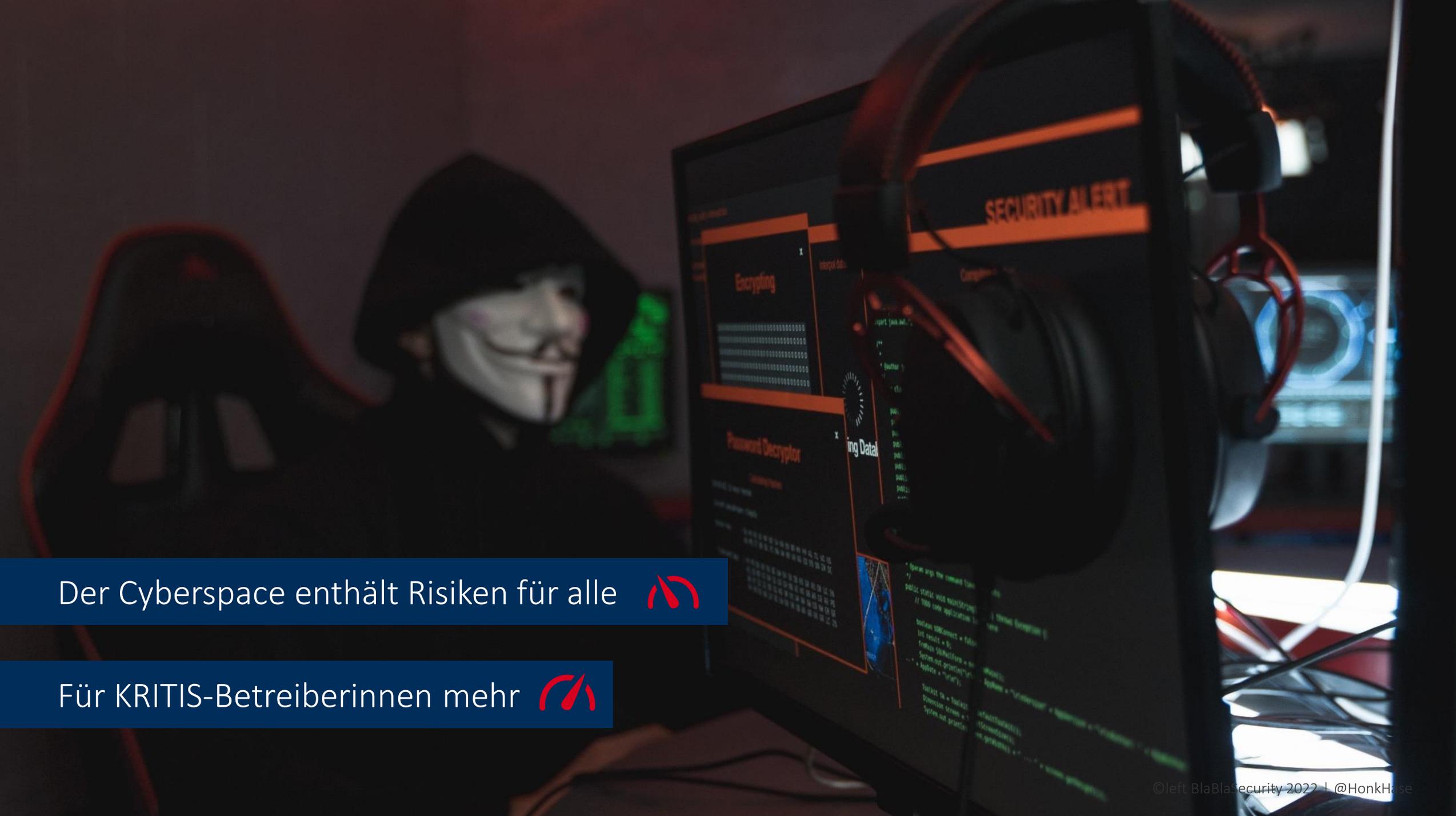
Quo vadis KRITIS?

- Primär **Schutz der Bevölkerung** (nicht des Betreibers)
- Enthalten oftmals **identische Komponenten**
- Immer mehr Komponenten werden **an das Internet verbunden**
- **OT** ist **Jahrzehnte** in **Betrieb** und **Einsatz!**

9 Kritische Infrastruktur Sektoren in der Schweiz

Der Bundesrat hat mit der nationalen SKI-Strategie 2018 - 2022 folgende Bereiche als kritische Infrastrukturen in der Schweiz festgelegt:

- Behörden
- Energie
- Entsorgung
- Finanzen
- Gesundheit
- Information und Kommunikation
- Nahrung
- Öffentliche Sicherheit
- Verkehr



Der Cyberspace enthält Risiken für alle 

Für KRITIS-Betreiberinnen mehr 

Wie sehen Cyber-typische Vorfälle aus?

- i.d.R. eher nicht langanhaltend, sondern temporär
- Wirtschaftliches Interesse (zB Ransomware)
- Spionage und Aufklärung
- Fake News und Propaganda
- Umfassende Kollateralschäden möglich, aber in der Risikoanalyse nicht kalkulierbar



Gibt es Bedrohungen für KRITIS!?

- Digitalisierung?
...schreitet bei KRITIS (langsam & schlecht) voran
- Ransomware wird mehr!
- Fachkräftemangel wird mehr!
- Naturereignisse werden mehr!
- Cyberwar-, Geheimdienste- & Hackback Szenarien bringen zukünftig mögliche Kollateralschäden



>> All-Gefahren-Ansatz <<

„Berücksichtigung aller Gefahrenarten
(z. B. Naturgefahren, technologische
Gefahren, etc.) im Rahmen des
Risiko- und Krisenmanagements“

** Hallo BBK*



Frage der Bevölkerung: Kommt morgen noch Strom & Wasser aus der Leitung?

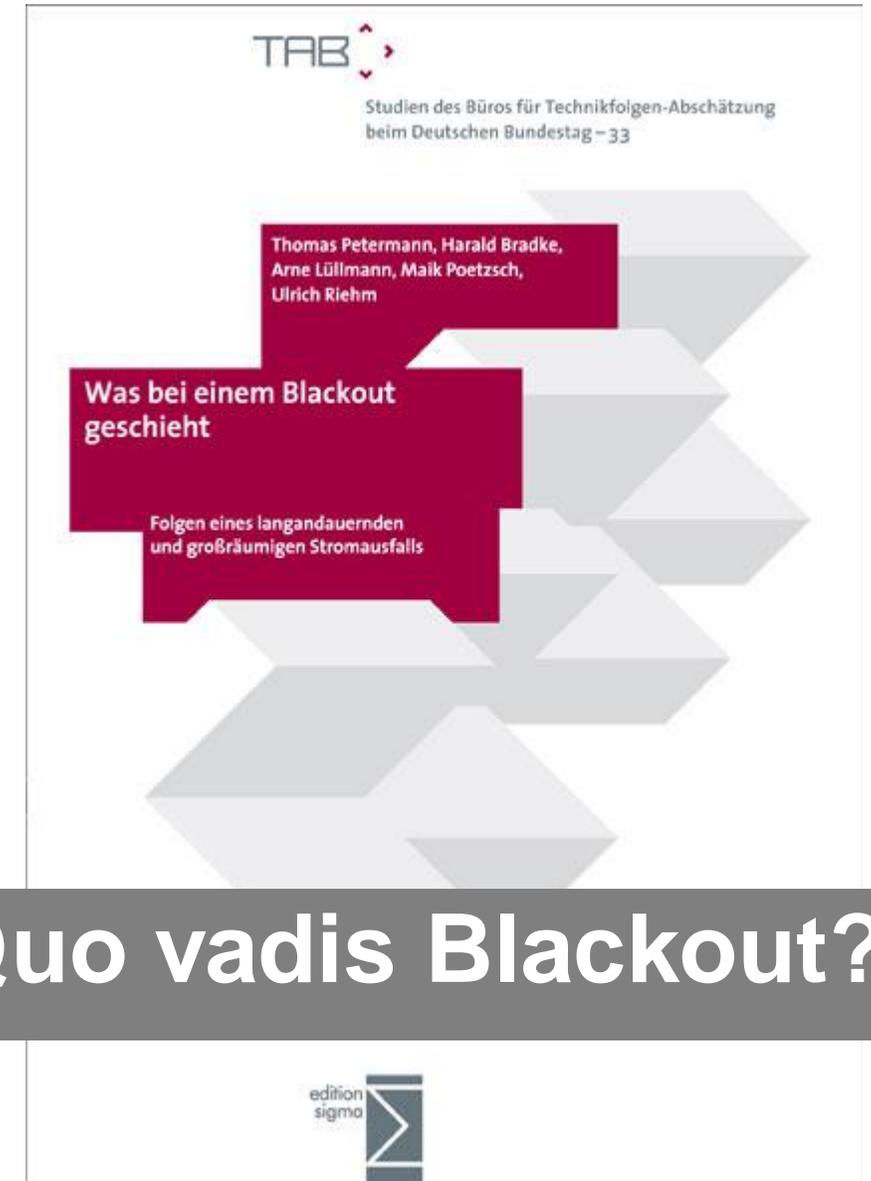
Blackout

Was bei einem Blackout geschieht:

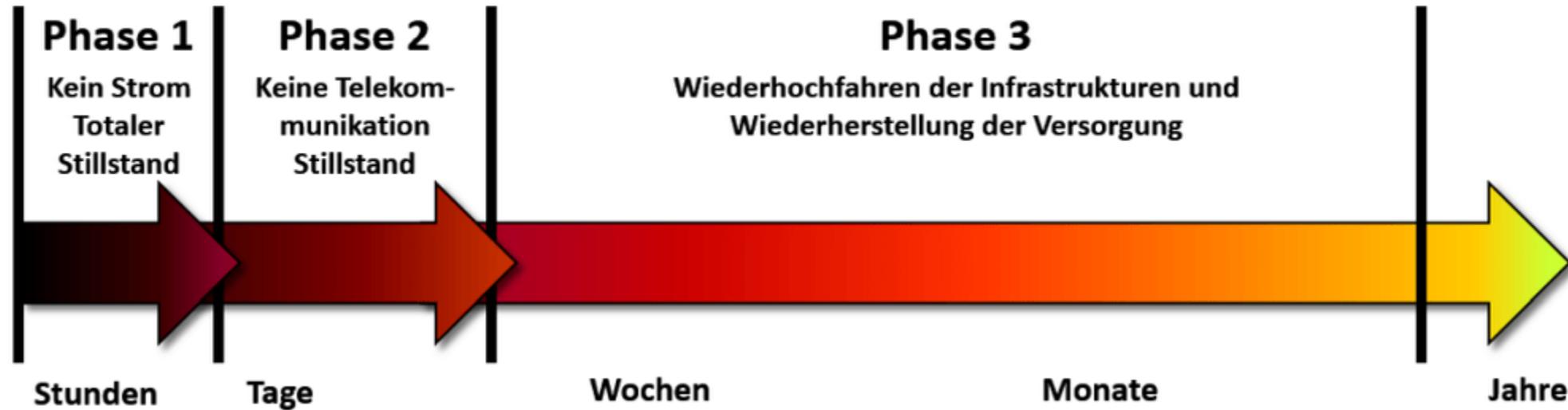
Folgen eines langandauernden und großflächigen Stromausfalls

Blackout != Stromausfall

<https://www.tab-beim-bundestag.de/news-2011-07-05-was-bei-einem-blackout-geschieht.php>



Die drei Phasen eines Blackouts



Quelle: Herbert Saurugg



KRITIS in Putins Angriffskrieg gegen Ukraine

Russischer Angriff auf Viasat KA-SAT



● Rat der EU Pressemitteilung 10. Mai 2022 11:44

Russische Cyberoperationen gegen die Ukraine: Erklärung des Hohen Vertreters im Namen der Europäischen Union

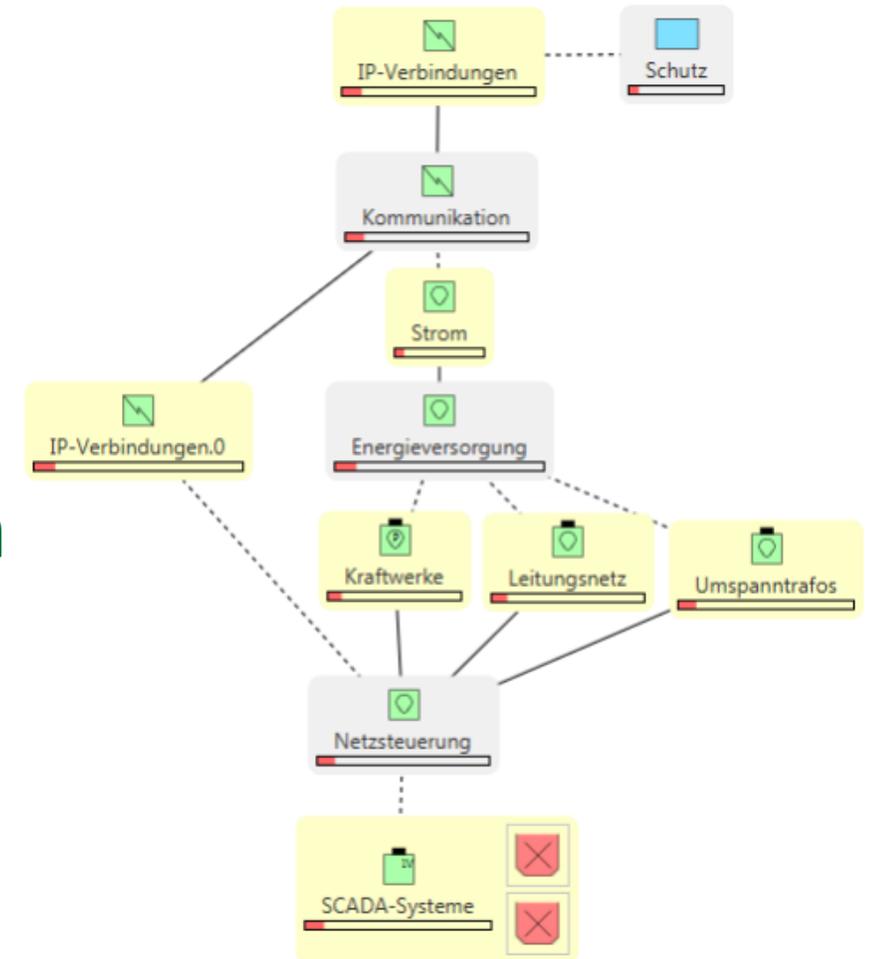
Die Europäische Union und ihre Mitgliedstaaten verurteilen gemeinsam mit ihren internationalen Partnern die böswilligen Cyberaktivitäten der Russischen Föderation gegen die Ukraine, die auf das Satellitennetzwerk KA-SAT von Viasat abzielten, aufs Schärfste.

- ~30 Min Kommunikationsausfall für Militär und Sicherheitsbehörden der Ukraine
- Kollateralschäden:
 - ~30.000 Modems Offline
 - ~5.800 Windkraftanlagen ohne Fernwartung
 - Ausfall ELW2 Katastrophenschutz Fahrzeuge

Cyber-Physische Auswirkungen auf KRITIS?

militärische Cyber-Wirkketten

- **Cyberwirkung** löst häufig eine Kettenreaktion auf dem **Fähigkeits-Ressourcen-Netzwerk** aus
 - Angriff auf **SCADA-System** führt zum Ausfall der **Stromversorgung**
 - Ausfall der **Stromversorgung** führt zum Ausfall der **Telekommunikation**
 - Ausfall der **Telekommunikation** führt zum Ausfall/Einschränkung von **Schutzfunktion**



KRITIS im Cyberraum ist sicher! Öhm...



Cyberresilienz & Ausblick

- Ursache für eine Katastrophe ist für die Bevölkerung nicht relevant
- Aber: eine Krise (Pandemie) in der Krise (Putins Angriffskrieg) in der Krise (Ransomware) in der Krise (Gasmangellage) in der **<beliebige Krise hier einfügen>** braucht keiner!
- Kritische Fragen:
 - Ist Digitalisierung immer erforderlich?
 - Können wir damit die Cyberresilienz von Produktionsumgebungen oder dem KRITIS Sektor Staat und Verwaltung erhöhen?
 - Was ist eine gute Digitalisierung?

Nachhaltigkeit in der Digitalisierung

- Bei der **digitalen Transformationen** verantwortungsvolle Maßnahmen einzuleiten und gewissenhaft durchzuführen, also zu operationalisieren, ist daher gleichsam eine **technische** wie **ethische Aufgabe!**
- Vermeidet daher **technische Schulden** an **kommende Generationen**
- Hinter jedem **Datensatz** steht ein **Mensch**
- **Security by Design** und **Privacy by Design** ist **Menschenschutz**

Und was mache ich, wenn alles nichts hilft?



Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspfluecker.de

