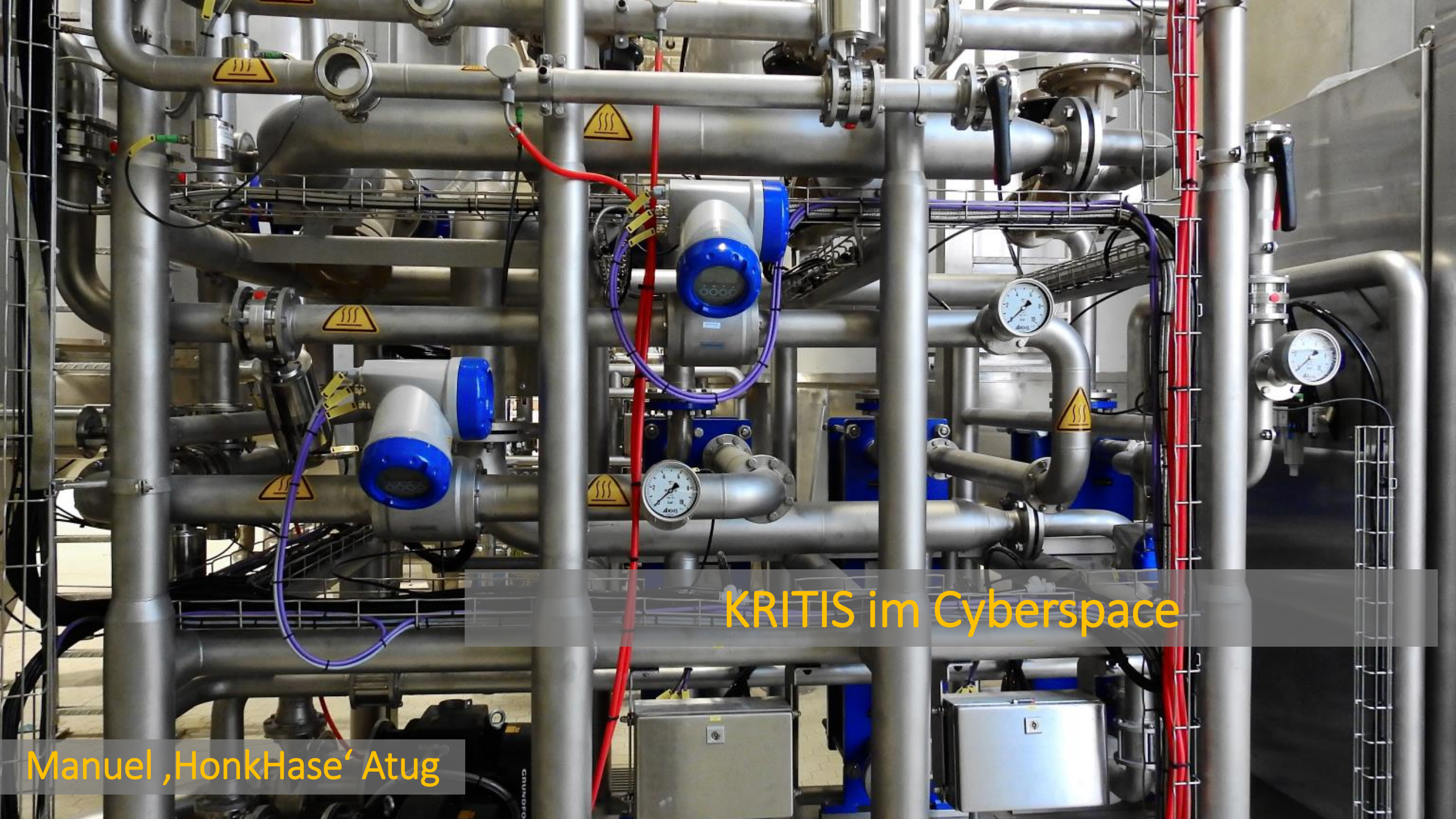
Kritische Infrastrukturen und Bevölkerungsschutz (KRITIS-BevS) TH Köln

Manuel ‚HonkHase' Atug



KRITIS im Cyberspace

Manuel ‚HonkHase‘ Atug

Manuel 'HonkHase' Atug

Principal bei der HiSolutions AG

- Diplom-Informatiker, Master of Science 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
- Experte der European Research Executive Agency (EU REA)
- Mitgründer der AG KRITIS: ag.kritis.info

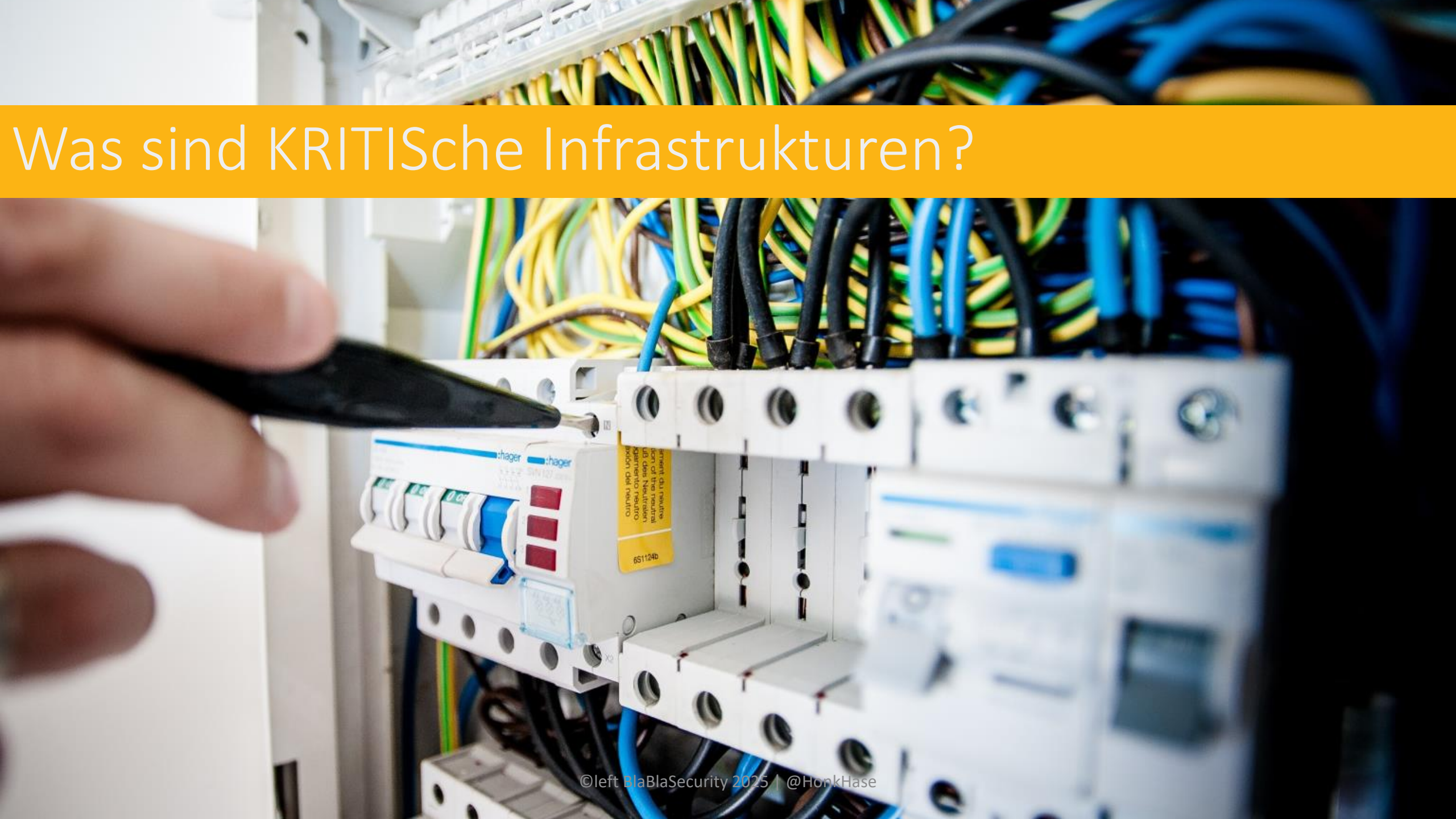
AG KRITIS

~~@HonkHase~~ @HonkHase@chaos.social

@honkhase.bsky.social

Ich habe #KRITIS im Endstadium

Was sind KRITISche Infrastrukturen?



Die 10 Kritische Infrastrukturen Sektoren in Deutschland

Quelle https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-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!

Wie ist Cybersicherheit in Deutschland organisiert?

Europäische Kommission

Your Europe
European Union

Single Digital Gateway: Einheitliches digitales Zugangstor zu den Verwaltungsleistungen der EU und der Mitgliedstaaten

EU-Mitgliedsstaaten

EU-Fristen einhalten. EU-Anforderungen mitdenken. EU-Komponenten nachnutzen.

Funktioniert das?

Bundeskanzleramt

Bundeskanzlerin
Chef des Bundeskanzleramtes
Staatsministerin für Digitalisierung

Gruppe Digitalpolitik, IT-Steuerung

Beide Projekte perspektivisch verbinden.

Digital Service 4Germany

dit.bund
DIT ist Innovation

Bundesministerium des Innern, für Bau und Heimat

Der Beauftragte der Bundesregierung für Informationstechnik

Bundesinnenminister
CIO der Bundesregierung

Abteilung Digitale Gesellschaft

Reicht der politische Wille?

BKAmt und BMI verantworten und koordinieren Umsetzung.

Monitoring auf solide Grundlage stellen! Orientierung geben!

Konferenz der Regierungschefinnen und Regierungschefs der Länder

Ministerpräsidenten

Chefs der Staats- und Senatskanzleien

Reicht der politische Wille?

Es braucht ein echtes politisches Controlling!

Die Bundesregierung

Digitalkabinett

Digitalrat der Bundesregierung

Vorschläge müssen umgesetzt werden.

daten ethik kommission

z.B. IMK WMK 2019

Fachministerkonferenzen

Reicht die Unterstützung?

Die Bundesregierung

IT-Konsolidierung Bund

IT-Rat

Informationstechnikzentrum Bund

ITZ Bund

Leistungs- und Unterstützungsfähigkeit muss erhöht werden.

FITKO

Zu wenig Personal!

unterstützen konzeptionell und operativ

KoSIT

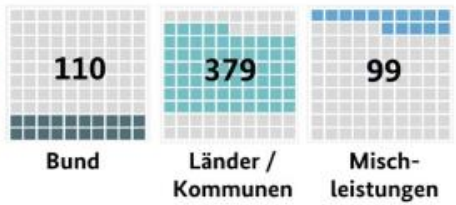
IT-Planungsrat

Bundes-CIO + Landes-CIOs
Kommunale Spitzenverbände

Zielsetzungen bis 2022

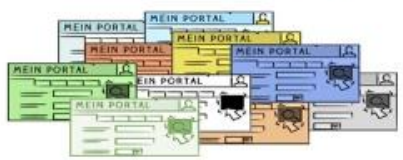
bis **2023**: Umsetzung **Single-Digital-Gateway-VO** (= EU-OZG)

1. Umsetzung der 588 **OZG-Leistungen**



2. Verknüpfung der Portale aller Ebenen zu einem **Portalverbund** (inkl. Servicekonten)

bund.de BETA Verwaltung digital



Bundesministerien

AA | BK | BMAS
BMBF | BMEL | BMF
BMFSFJ | BMG | BMI
BMJV | BMU | BMVI
BMVG | BMWi | BMZ

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Datenschutzfragen zu Registern und Datencockpit klären.

Datenschutzfragen zu Registern und Datencockpit klären.

DSK Landes-Datenschützer

IT-Dienstleister der Länder & Kommunen

IT-Unternehmen, Start-Ups

Länder und Kommunen

294 Landkreise, ca. 11.000 Gemeinden

Deutscher Städtetag | DStGB | Deutscher Landkreistag

Prinzipien

Digital First
(digitale Verfahren als Regelfall)

Once Only
(Daten nur noch einmal angeben)

Transparenz verbessern!

Bund, Länder und Kommunen entwickeln gemeinsam Lösungen.

Privates IT-Know-How besser einbinden! FIT-Store-Konzept anpassen.

Bund gibt zusätzlich 3 Mrd. Euro!

Flächendeckung fraglich! Es bleiben nur noch 2 Jahre Zeit!

Sind alle nötigen Mittel eingeplant (**1,5 Mrd. Euro**)?

KRITIS Sektor Staat und Verwaltung digital handlungsfähig?

Die staatliche Cybersicherheitsarchitektur Deutschlands ➔

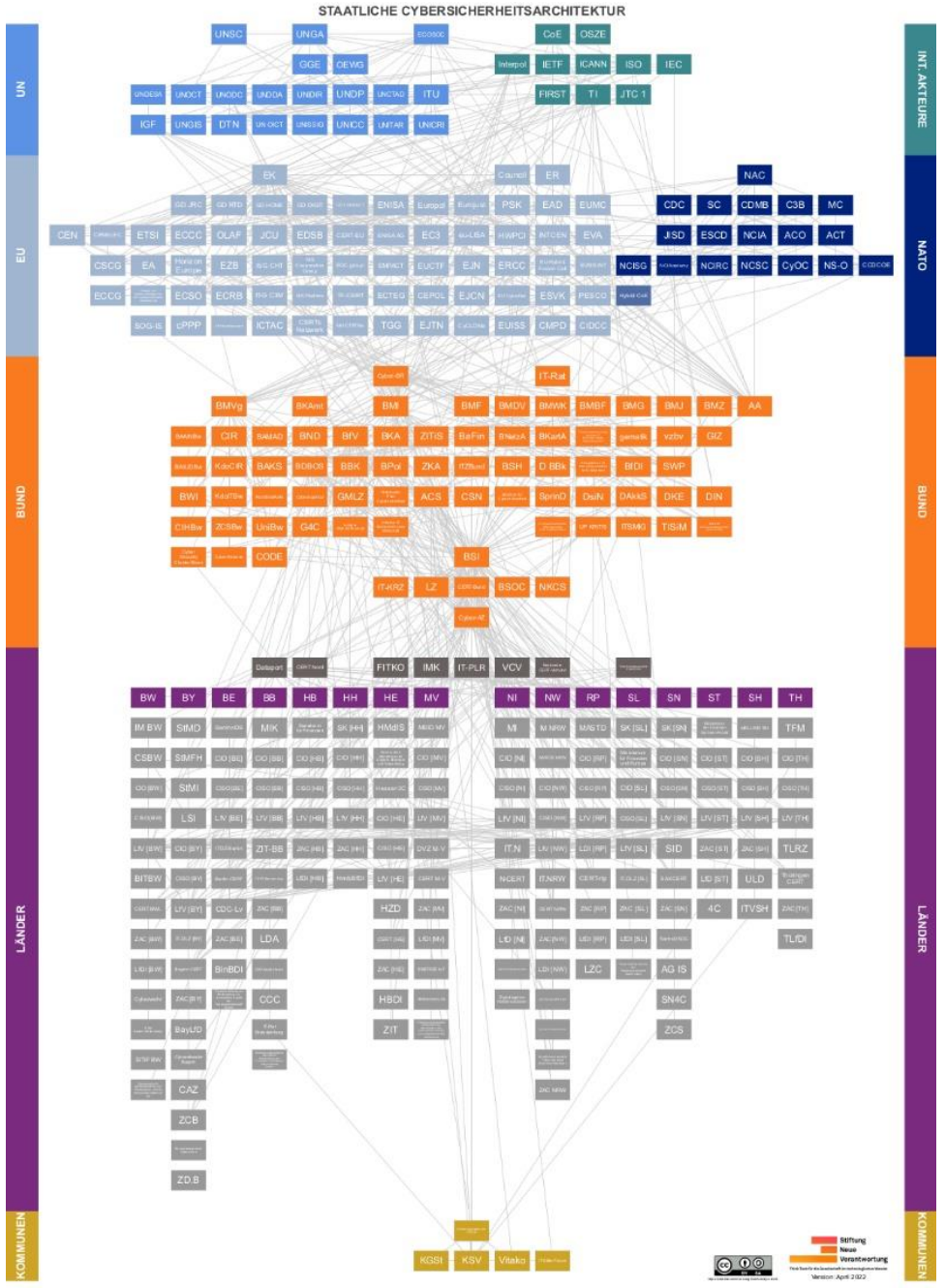
UN

Europe

Germany

Federal States

Municipalities



Int. Actors

NATO

Germany

Federal States

Municipalities

Gesetzeskarte für das Energie-versorgungs-system

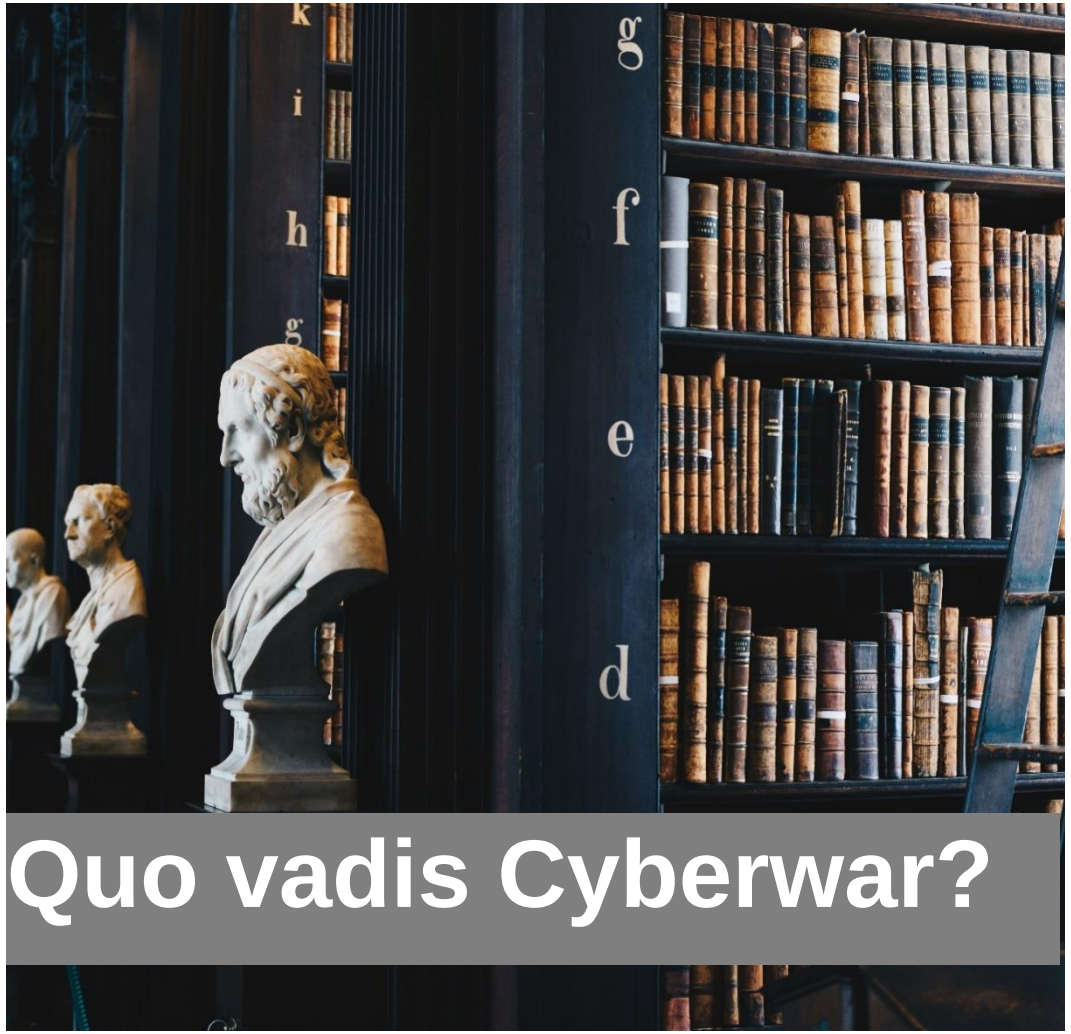
(Karte zentraler Strategien, Gesetze und Verordnungen)

How to Cyber: Prävention | Detektion | Reaktion

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Gibt es einen Cyberwar? Was ist das?

Zyberkrieg?



Krieg ist ein **Akt der Gewalt**, um beim Gegner einen (politischen) **Willen zu erzwingen**

Krieg gegen Terrorismus, Handelskrieg und Cyberwar sind also:

>> keine Kriege im eigentlichen Sinne <<

Hybrid Warfare, Information Warfare & Cyberwar (I)

„…die hybride Kriegsführung beschreibt eine flexible Mischform der offen und verdeckt zur Anwendung gebrachten regulären und irregulären, symmetrischen und asymmetrischen, militärischen und nicht-militärischen Konfliktmittel mit dem Zweck, die Schwelle zwischen den völkerrechtlich angelegten binären Zuständen Krieg und Frieden zu verwischen.“

Quelle: Wikipedia

Hybrid Warfare, Information Warfare & Cyberwar (II)

„…information warfare…ist eine Bezeichnung für die gezielte Nutzung und Manipulation von gesteuerten Informationen, um in der Wirtschaft oder in der Politik Vorteile gegenüber Konkurrenten und Gegnern zu erzielen. Dazu gehört auch die Beeinflussung von Medien durch Falschinformationen (Fake News), Teilinformationen oder Propaganda mit dem Ziel der Medienmanipulation im eigenen Interesse.“

Quelle: Wikipedia

Zybervorfälle, Information Warfare & Hybrid Warfare!

Cybervorfälle haben eher andere Motive

- Cybercrime

  (wie Ransomware)

- Cyberspionage und Aufklärung

  (ja, auch unter Freunden & in Friedenszeiten)

- Subversion

  (Beeinflussung durch Propaganda und Fake News)

Die Dimensionen im Militär

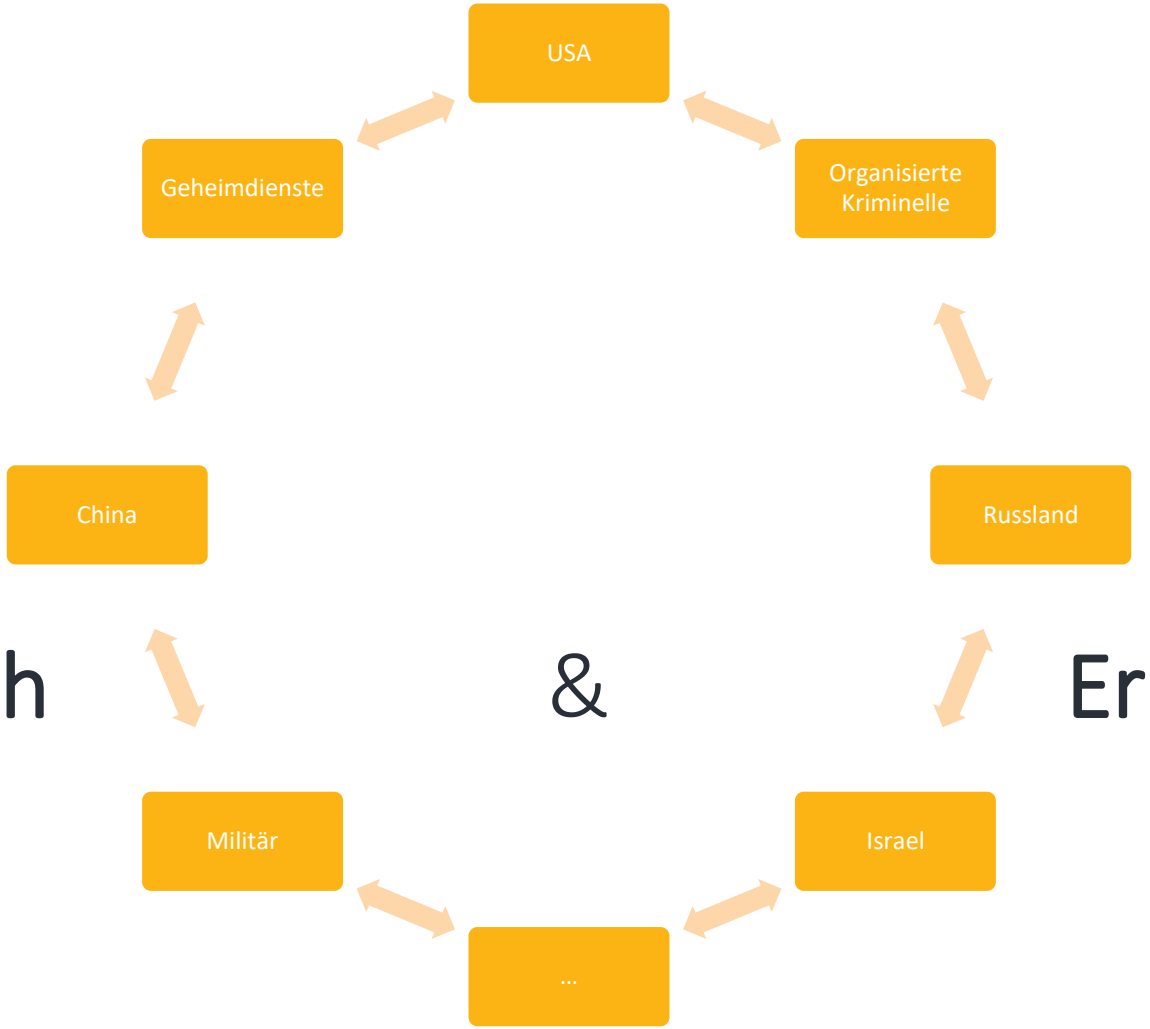
Ziel militärischer Cyber-Operationen im Hybrid Warfare

(durch militärischen Operationen „zur Aufklärung und Wirkung“)

- Cyber-Operationen
  - **Spionage**
  - **Beeinträchtigung** der Führungsfähigkeit
  - **Sabotage** Kritischer Infrastrukturen (KRITIS)
  - **Defacement** von regierungseigenen Webseiten und offiziellen Kommunikationswegen
  - **Desinformation** über soziale Medien
  - **Blockade** des nationalen Zugangs zum Internet

Organisierte Kriminalität, Geheimdienste und andere staatliche Akteure

Schutz vor was und wem?



Machtmissbrauch & Erlösmaximierung

KRITIS in Putins Angriffskrieg gegen Ukraine

Es herrscht Krieg, aber ist das auch ein Cyberwar?

Cyberwar? Gübt’s hür nücht!

- Ja, das BMI nennt es „massive Cyberangriffe“
- Es waren eher Defacements und DDoS Angriffe auf Ministerien und Banken
- Joah, es gab auch 5 Wiper Angriffe
- KA-Sat Angriff auf Sateliten-Kommunikation
  ~30 Min Kommunikationsausfall
  Dafür Kollateralschäden:
  - ~30.000 Modems Offline
  - ~5.800 Windkraftanlagen ohne Remote Acces
  - Ausfall ELW2 Katastrophenschutz Fahrzeuge

(Nicht-Cyber-)Sabotage!!! Überall!!!

Pipelines und Glasfaser-Kommunikation bei der Bahn

- Es braucht Ressourcen
- Es braucht ein Motiv und die Motivation
- Es braucht die Durchführung als Wille

- Es braucht zur Verhinderung nicht:
  - 1.000 weitere Bundespolizeibeamte
  - Überwachung von <EinmalAllesGanzViel>

Cyberwar vs. Realität

Der Cyberwar findet auf PowerPoint-Folien statt,
in der Realität ist es ein Krieg der Bomben und Granaten

Russischer Angriff auf Viasat KA-SAT

Cyberwehr
Wir. Dienen. Neuland.

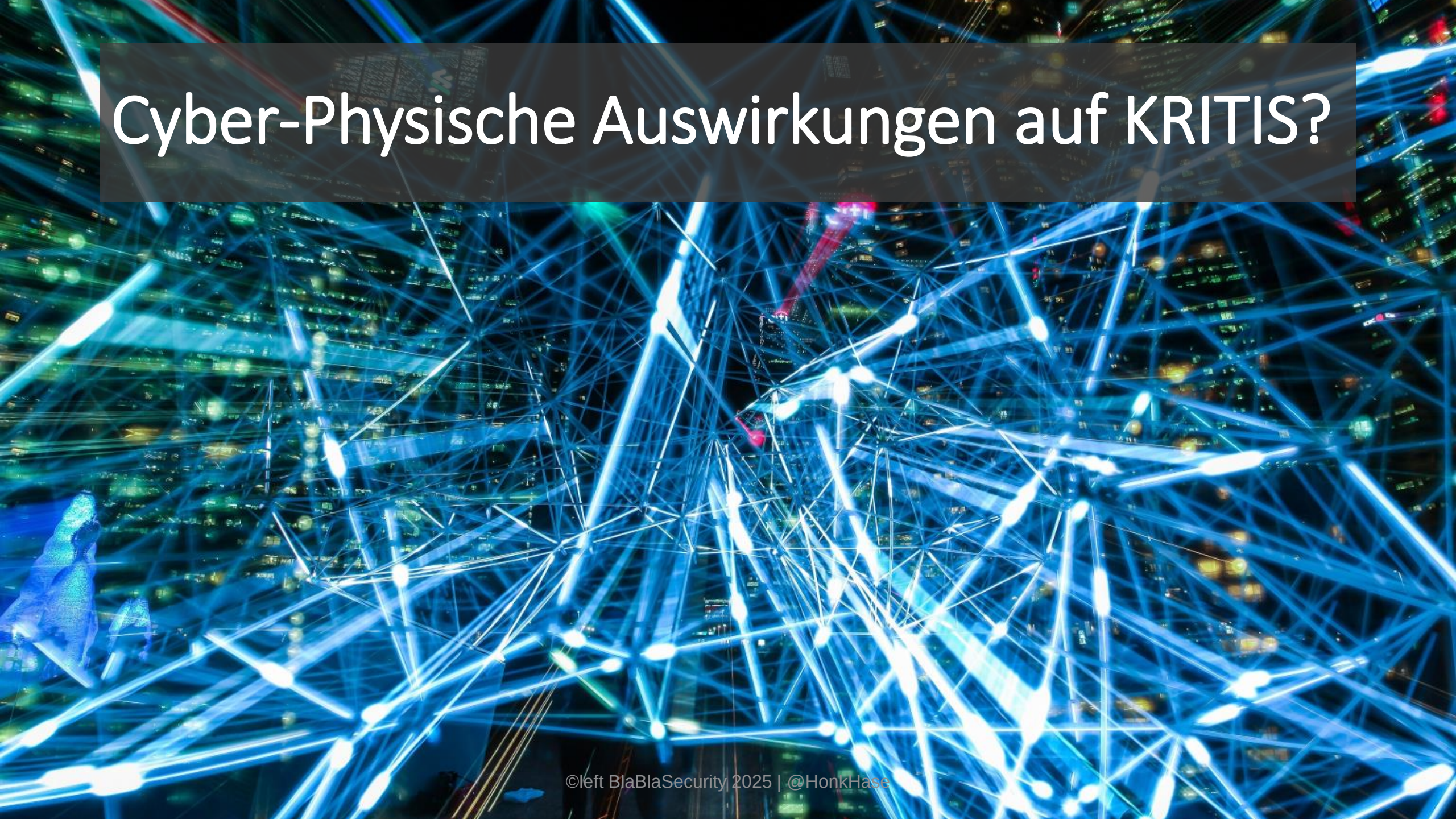
Rat der EU Pressemitteilung 10. Mai 2022 11:44

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

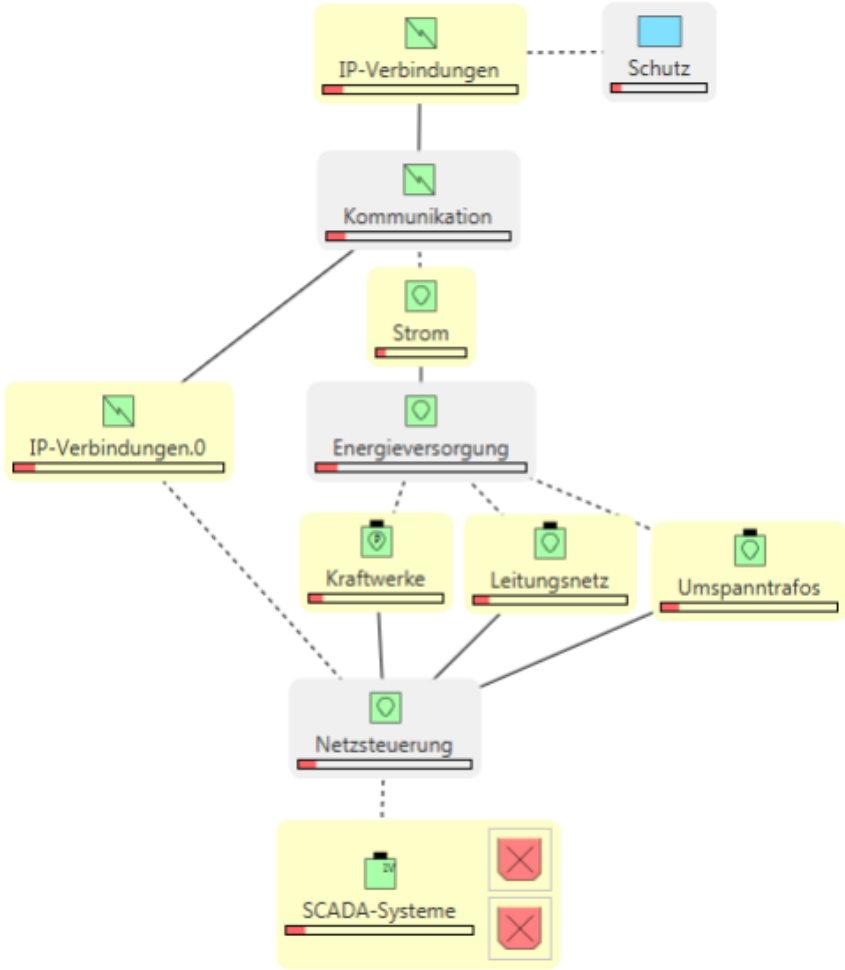
Cyber-Physische Auswirkungen auf KRITIS?



militärische Cyber-Wirkketten

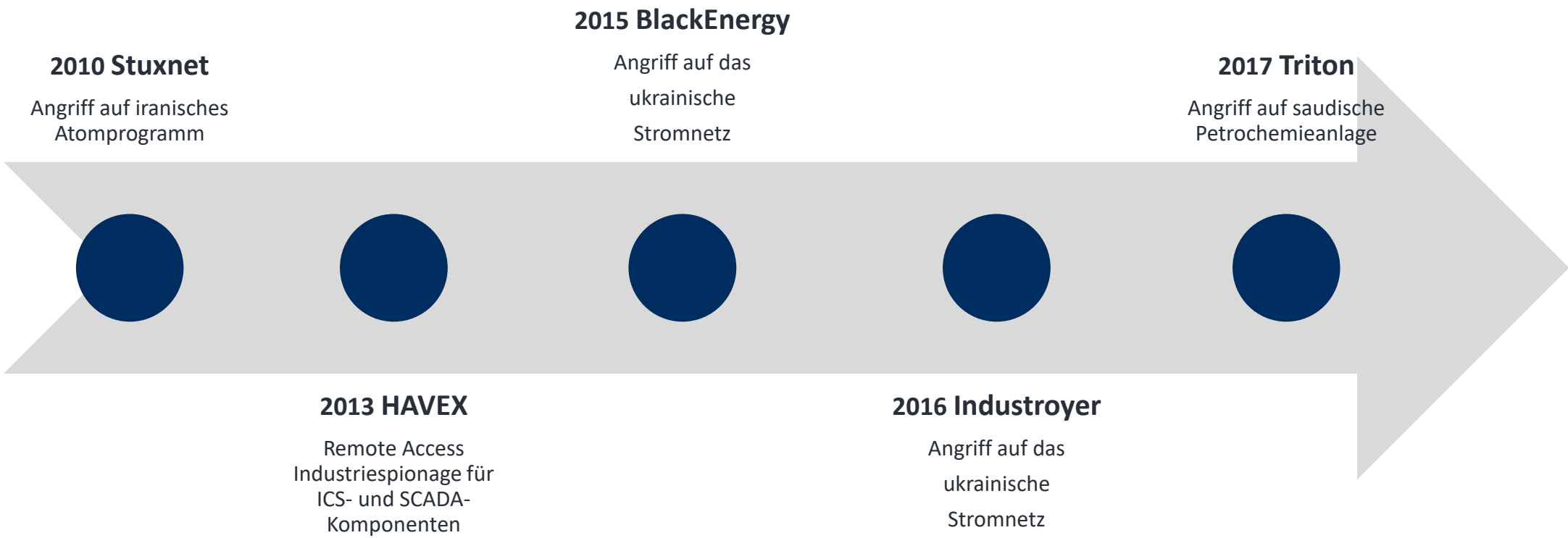
(Theorie)

- **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**



Timeline der wesentlichen ICS Angriffe

(Und welche davon waren Cyberwar?)



Realitätsabgleich

(Praxis)

Ja aber wir haben doch viele Millionen Cyberangriffe am Tag!!!eins!!elf!

Portscan != Angriff
Cyberangriff != Cyberwar
Hype und Angst != Cyberrealität

2 x Stromausfall in Ukraine!

Stromausfall != Blackout

Es gibt Cyber-physische Vorfälle!

- * Stuxnet
- * Projekt Aurora

Beide keine Kriegsoperation

* Sabotage durch Geheimdienste

* Wissenschaftliches Experiment

Projekt Aurora - Cyber-physischer Proof of Concept

Ist ein alter Hut

Aurora Generator Test am Idaho National Laboratory in 2007

*“The experiment used a **computer program** to **rapidly open and close** a diesel generator's **circuit breakers** out of phase from the rest of the grid and cause it to **explode**”*

Quelle: https://en.wikipedia.org/wiki/Aurora_Generator_Test

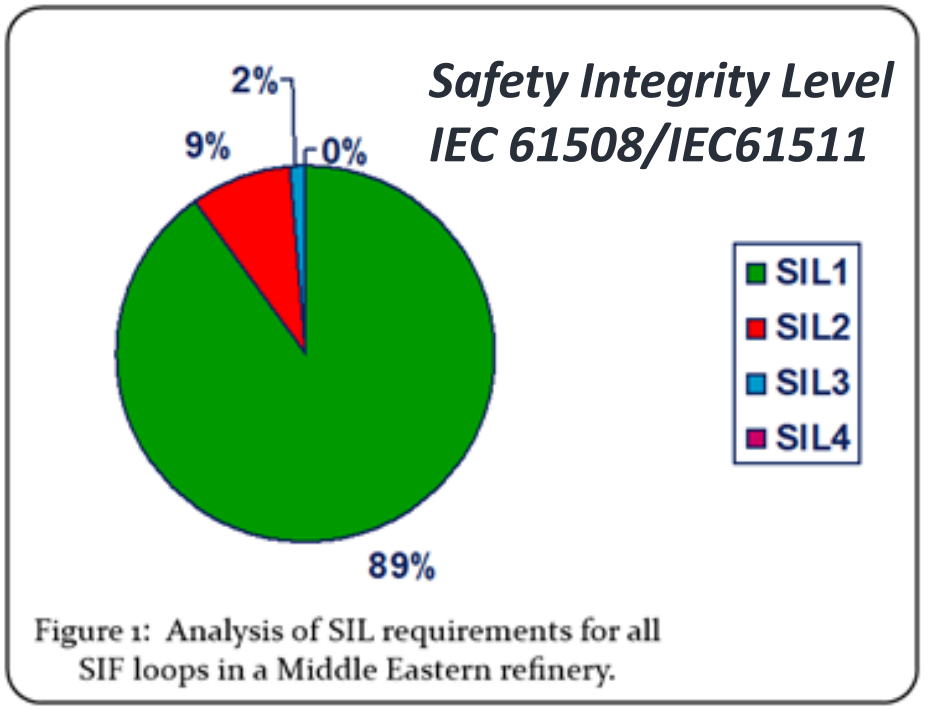


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.

Triconex Tricon

Attacke auf Saudi Arabisches Petrochemiewerk

- TRITON: passiver Implant mit Remote Access Funktion
- Folge wäre gewesen: Explosionen und die Freisetzung von Schwefelwasserstoffgas

Safety-PLC gemäß Safety Instrumented System (SIL3)
Firmware wurde im RAM gezielt manipuliert

Gibt es denn 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

Staatliche und nicht-staatliche Akteure im Cyberraum

Es gibt nur einen gemeinsamen Cyberraum für alle. Ja, auch im Krieg!

- Militär - und damit Cyber-Kombattanten
- Geheimdienste - könnten überall dahinter stecken
- Cybercrime – Ransomware & Co
- Kritische Infrastrukturen inkl. Staat und Verwaltung
- Wirtschaft, Wissenschaft & Forschung
- Zivilgesellschaft: Bürgerinnen; ethisch noch nicht gereifte Jugendliche; destruktive „Cyber-Hooligans“; Hackerkollektive wie Anonymous

Cyber-Verteidigung

(it‘s all about Cyber…)

Wie? Das ist doch quasi Magie… wie KI oder Blockchain…

Cyberresilienz! Zur Erhöhung der Widerstandsfähigkeit von KRITIS

** Fähigkeit eines Systems, Ereignissen zu widerstehen bzw. sich daran anzupassen und dabei seine Funktionsfähigkeit zu erhalten oder möglichst schnell wieder zu erlangen*

Warum? Angriffe verpuffen wirkungslos durch Basis-Maßnahmen

** Hallo, BSI Grundschutz*

How to Backup

(…die langweiligen Basics der IT-Security)

- Habt ihr ein Backup erstellt?
- Ist es frisch oder fermentiert es vor sich hin?
- Habt ihr das sogar Offline vorliegen?
- Habt ihr mal die Wiederherstellung getestet?

Denkt dran:

- Cloud Speicher ist kein Backup!
- Beim KFZ fragt man auch die Werkstatt

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

Cyberresilienz ➔ Widerstandsfähigkeit gegen Ereignisse

- Ursache für Katastrophe oder Cybervorfall 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 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 ➔ Daten können toxisch sein
- Security by Design und Privacy by Design ist Menschenschutz

>> All-Gefahren-Ansatz <<

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

** Hallo BBK*

Und was mache ich, wenn alles nichts hilft?

Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspflücker.de