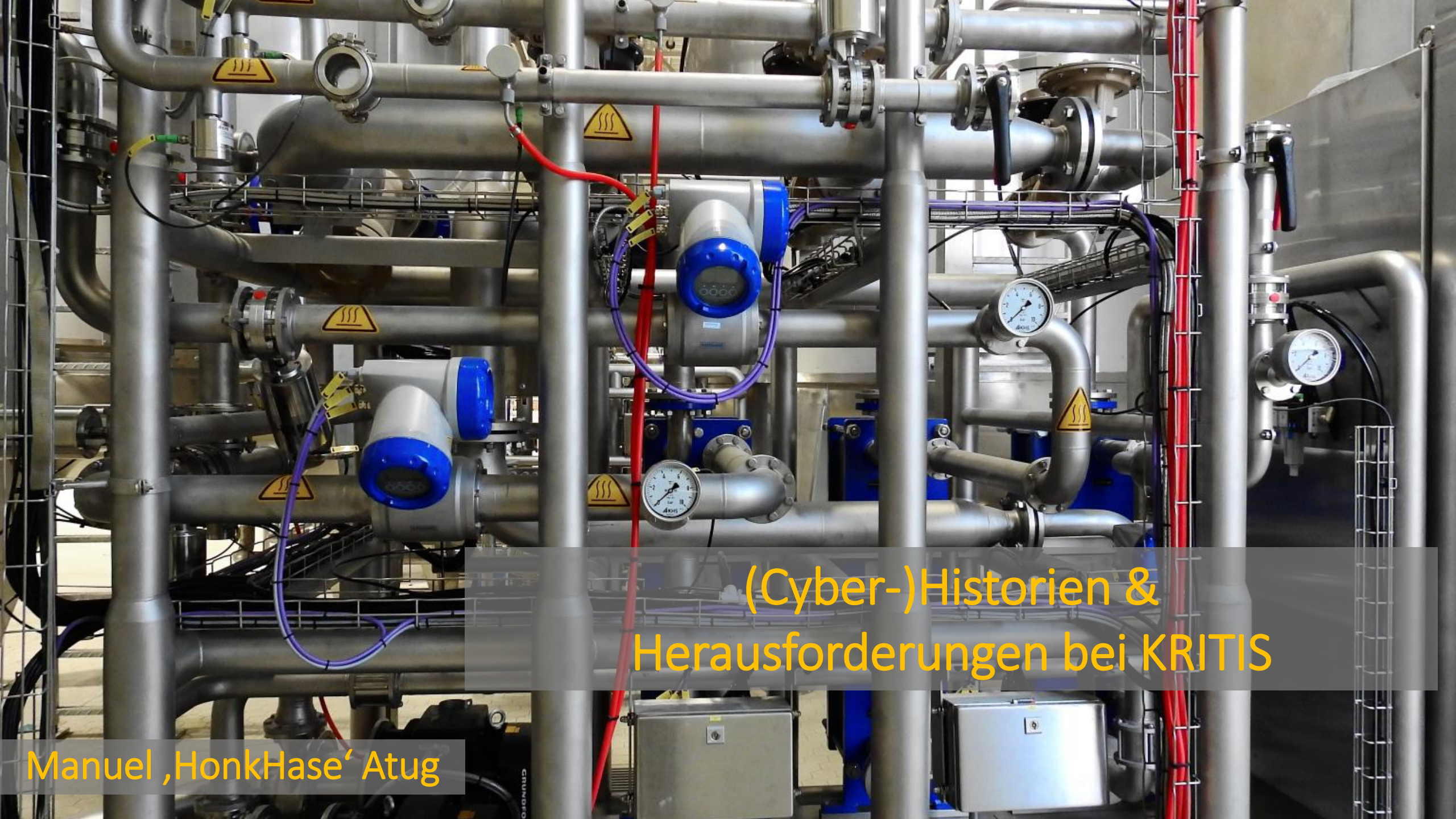


A black and white photograph of an industrial facility, likely a refinery or chemical plant. The image shows a complex network of large pipes, metal walkways with railings, and various industrial structures in the background. The perspective is from a walkway, looking down a corridor of pipes and structures.

ZOES Morgenlage

Manuel „HonkHase“ Atug



(Cyber-)Historien & Herausforderungen bei KRITIS

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



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

 [@honkhase.bsky.social](https://bsky.social/@honkhase)

Ich habe #KRITIS im Endstadium



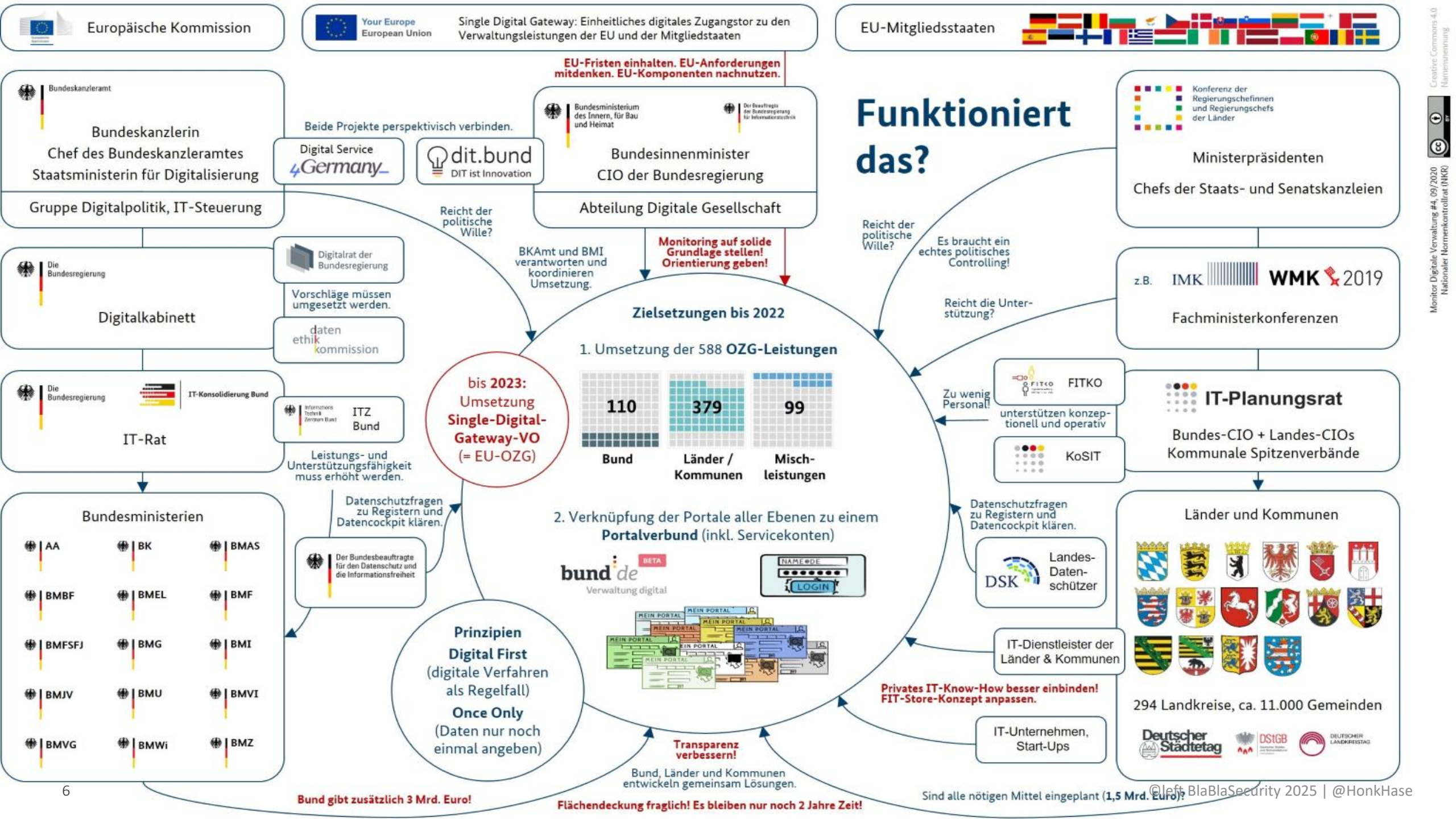


Quo vadis KRITIS?

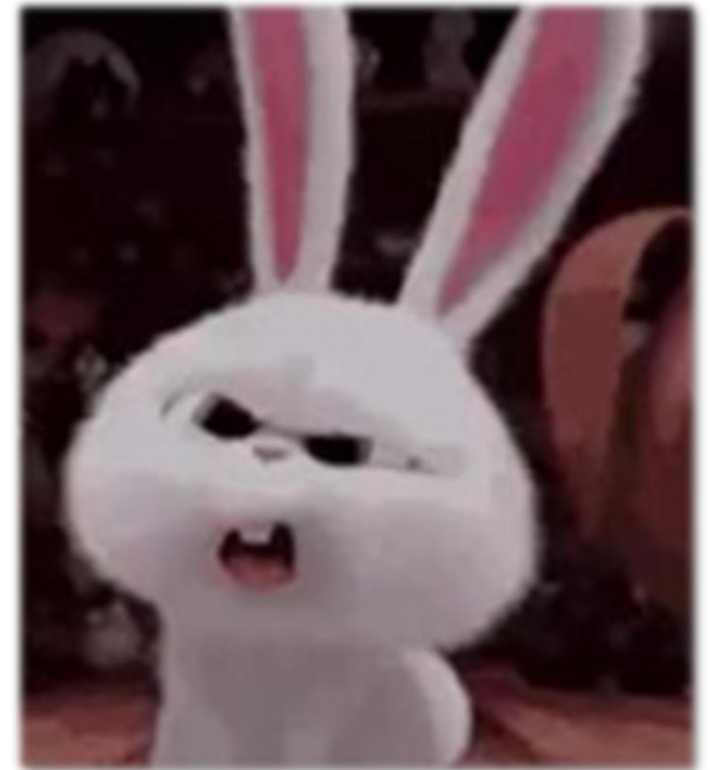
- Primär **Schutz der Bevölkerung** (nicht des Betreibers)
- Enthalten oftmals **identische Komponenten**
- Immer mehr Komponenten werden **an das Internet verbunden**
- **OT** ist **Jahrzehnte** in **Betrieb** und **Einsatz!**



Verwaltung & Cybersicherheitsgesetzgebungen



KRITIS Sektor Staat und Verwaltung digital handlungsfähig?



Die staatliche Cybersicherheitsarchitektur Deutschlands →

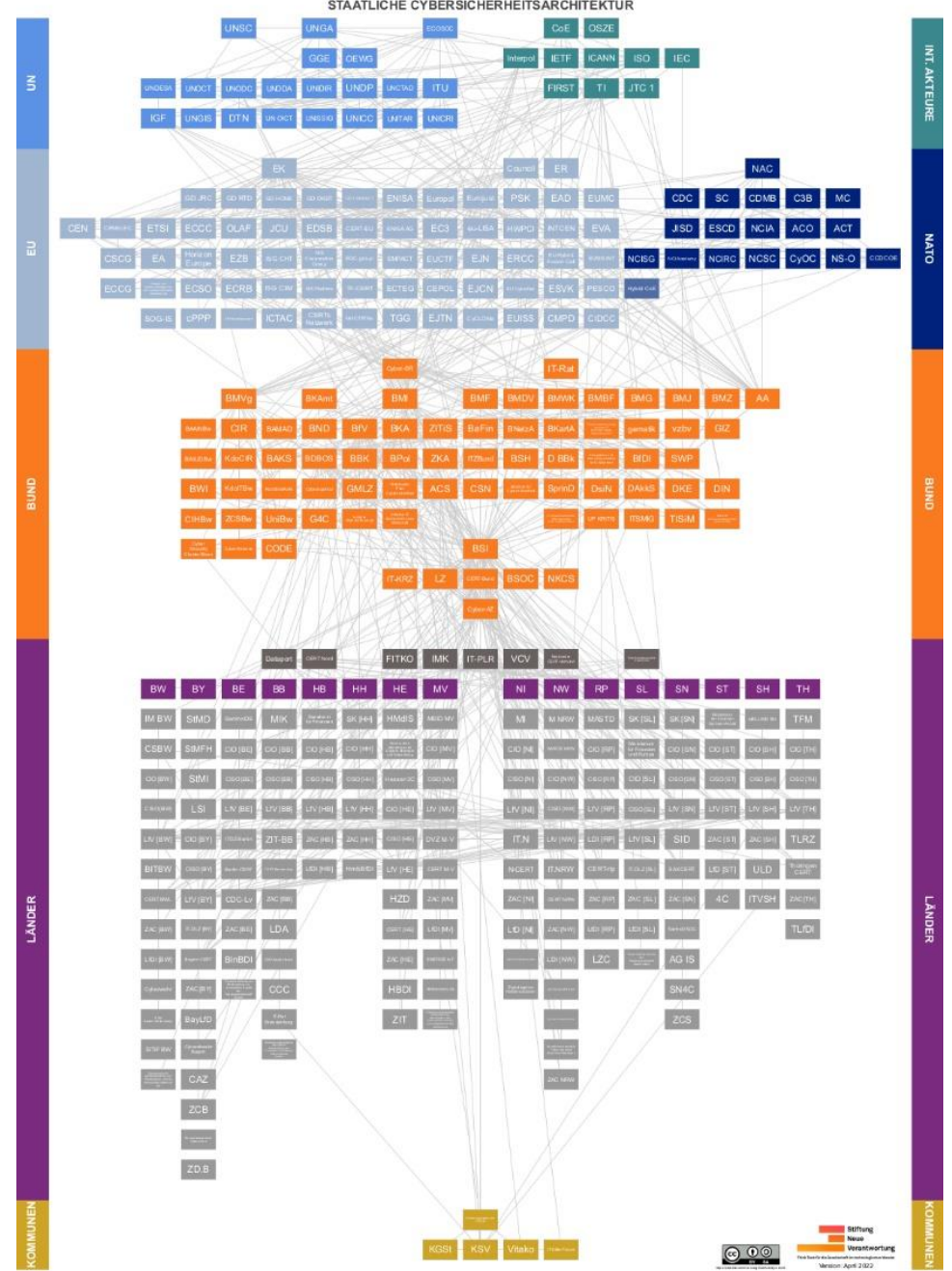
UN

Europe

Germany

Federal States

Municipalities



Municipalities

Federal States

Germany

Int. Actors

NATO

(naja, so ein bisschen halt)



Cyberdiarrhö





Offensive Lösungen

- Schon drölfzehn Mal verstorben:
 - Zombie Vorratsdatenspeicherung
- Sicherheitspaket
 - Massenüberwachung
 - Gesichtserkennung
 - Anlasslose Kontrollen
 - Wo ein Trog, da kommen...
- Wer uns ancybert, wird weggecybert
 - Hackback (manchmal auch Hackfirst)
- Schwachstellenmanagement
 - Verwalten (und ausnutzen) statt beheben



- Unhackbar! (by Law, nicht by Design)
 - nationale Sicherheit
 - öffentliche Sicherheit
 - Verteidigung & Militär
 - Kommunen
 - Landkreise
 - Strafverfolgungsbehörden
 - Geheimdienste

Zeitenwende

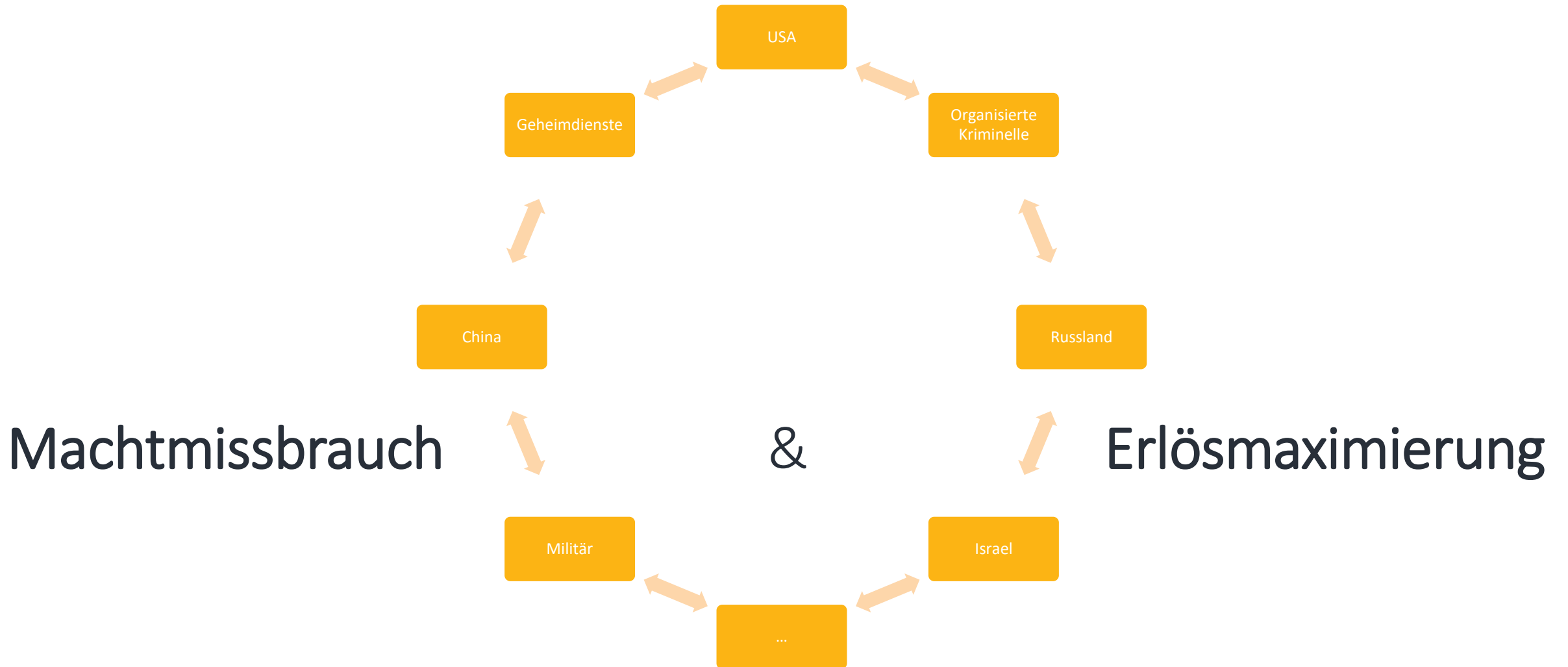
(angekündigt)



Organisierte Kriminalität, Geheimdienste und andere staatliche Akteure



Schutz vor was und wem?



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





Dinge beim Namen nennen

Was ist KI?



- KI ist Software (und ganz viel Daten)
- Software kann man sicher entwickeln und betreiben. Oder eben auch nicht
- Software kann nicht denken

Wie nutze ich KI?



- Technologiehörigkeit vs Heilsversprechen
- Mittel zum Zweck vs Selbstzweck



Verlust der digitalen Souveränität über 3 Langzeit-Etappen



Hardware

- Speicherung der Daten
- Externe RZ Konzerne



Applikationen

- Verarbeitung der Daten
- Externe Cloud Konzerne



Daten

- Abgabe der Daten
- Externe KI Konzerne



>> All-Gefahren-Ansatz <<

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

** Hallo BBK*



Cyberwar vs. Realität

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

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

Resilienz ist das Mittel zum Zweck

(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 (ISMS mit BCM)*

Bedrohungen und Gefährdungen

- **Und alle: Cloud & KI**
- Was ist mit staatlichen Systemlandschaften?
- Was ist mit Betriebssystemen und Smartphones?
- Was ist mit Netzwerkequipment und Firewalls?
- Was ist mit Systemen zur Angriffserkennung?



Lieferkette: Israel XM Cyber



Ex-Mossad-Chef Tamir Pardo gründete ein Start-up, das Banken, Firmen und Regierungen berät.

Foto: picture alliance / dpa

SICHERHEIT

»Tödlich wie die Atombombe«

Tamir Pardo warnt davor, das Zerstörungspotenzial von Cyberkriminellen zu unterschätzen

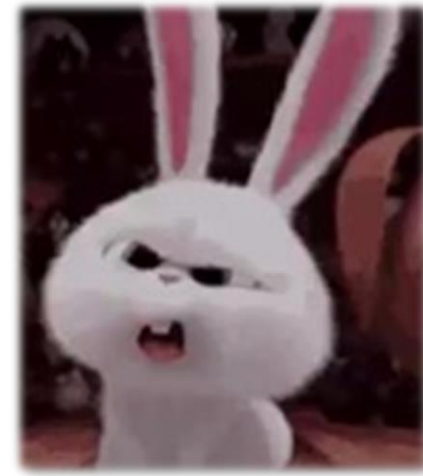
von Pierre Heumann

🕒 14.02.2021 11:06 Uhr

Von 2010 bis 2015 war er Direktor des Mossad.

Nach seinem Ausscheiden aus dem Geheimdienst vor fünf Jahren gründete er, zusammen mit zwei weiteren Ex-Mossad-Agenten, die Cyberfirma »XM Cyber«. Das Start-up hat eine vollautomatische Simulationsplattform für anhaltende Bedrohungen entwickelt, um Angriffe kontinuierlich aufdecken und den Handlungsbedarf lokalisieren zu können. Es zählt unter anderem Banken, Versicherungsfirmer, Flughäfen, Energiefirmer, Regierungen, Logistikfirmer und Börsen zu seinen Kunden.

Der Endgegner der Souveränität: Palantir



- Autokratie-Etablierung durch Peter Thiel
- auch durch deutsche Steuergelder
- mittels deutscher Strafverfolgungsbehörden & Geheimdiensten
- USA als „CEO geführte Firma“ ohne Regulierung
- Vorstufe „Freedom Cities“
- Freiheit nicht mit Demokratie vereinbar



CyberCyber in der Lieferkette aka Systeme zur Angriffserkennung

- SzA vs. Antivirus vs. End Point Protection
- Alles oder nix?
 - Systemrechte und Vollzugriff oder zB passiv am Netzwerk?
- On-Prem oder in der Cloud?
 - Datenexport oder Souverän?
- Deutschland vs. USA vs. Israel?
 - Ist doch alles das gleiche Cyber?
- Sammeln und analysieren vs. Software Entwicklung vs. AGBs
- Crowdstrike vs Kaspersky vs. XM Cyber von Schwarz Gruppe / Schwarz Digits





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.kokosnusspfluecker.de

