4. Regensburger Cybersecurity Kongress

Manuel ‚HonkHase‘ Atug

Weggecybert durch falsche OT-Security?!

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

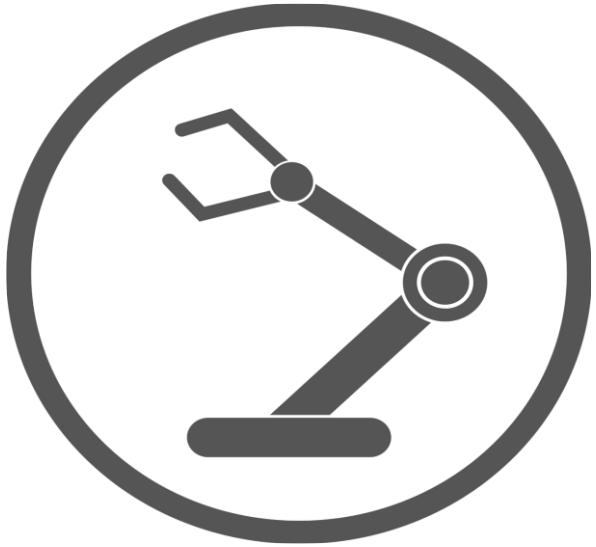
Ich habe #KRITIS im Endstadium

IT vs. OT

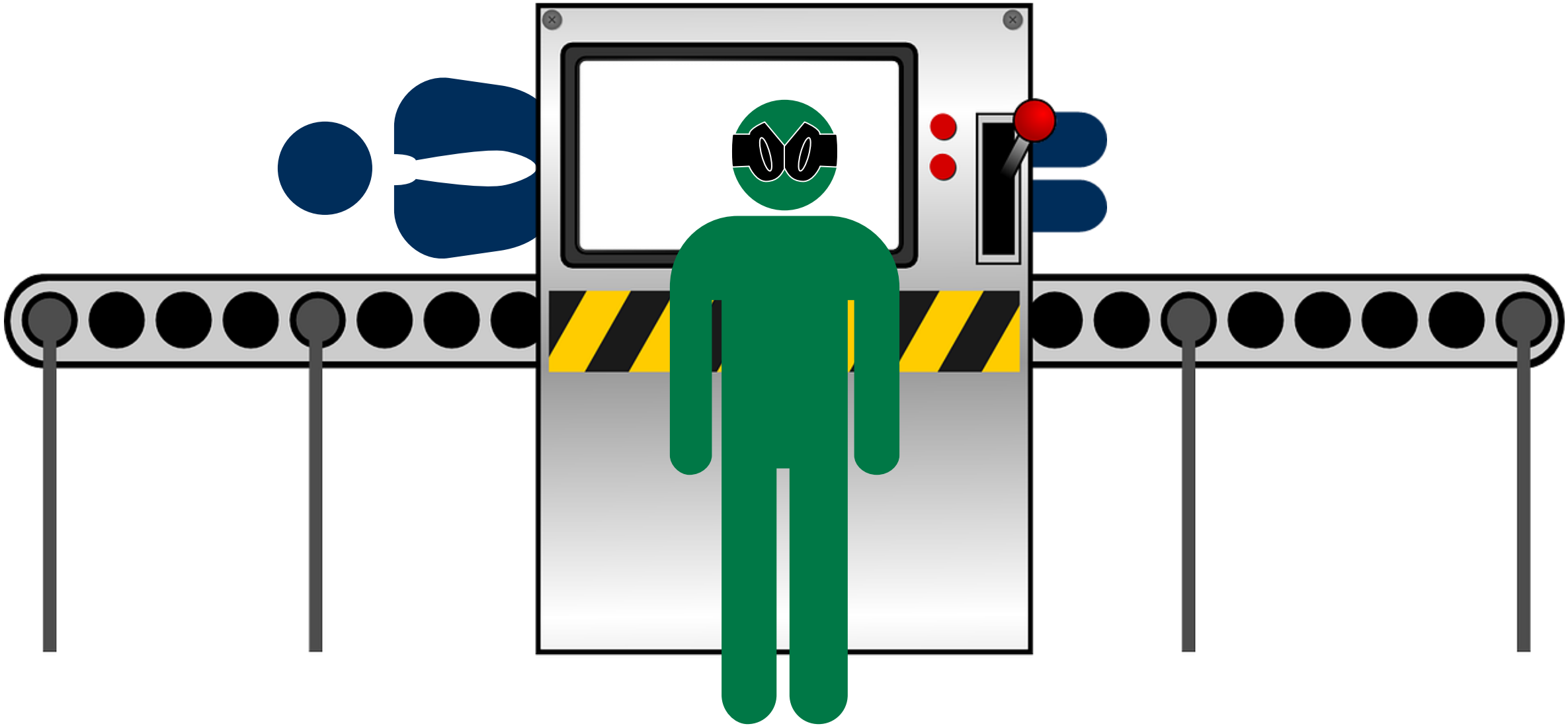
> Safety schützt Menschen (und Umwelt) vor Maschinen,
> Security schützt Maschinen vor Menschen

Fluchs, S. 2020

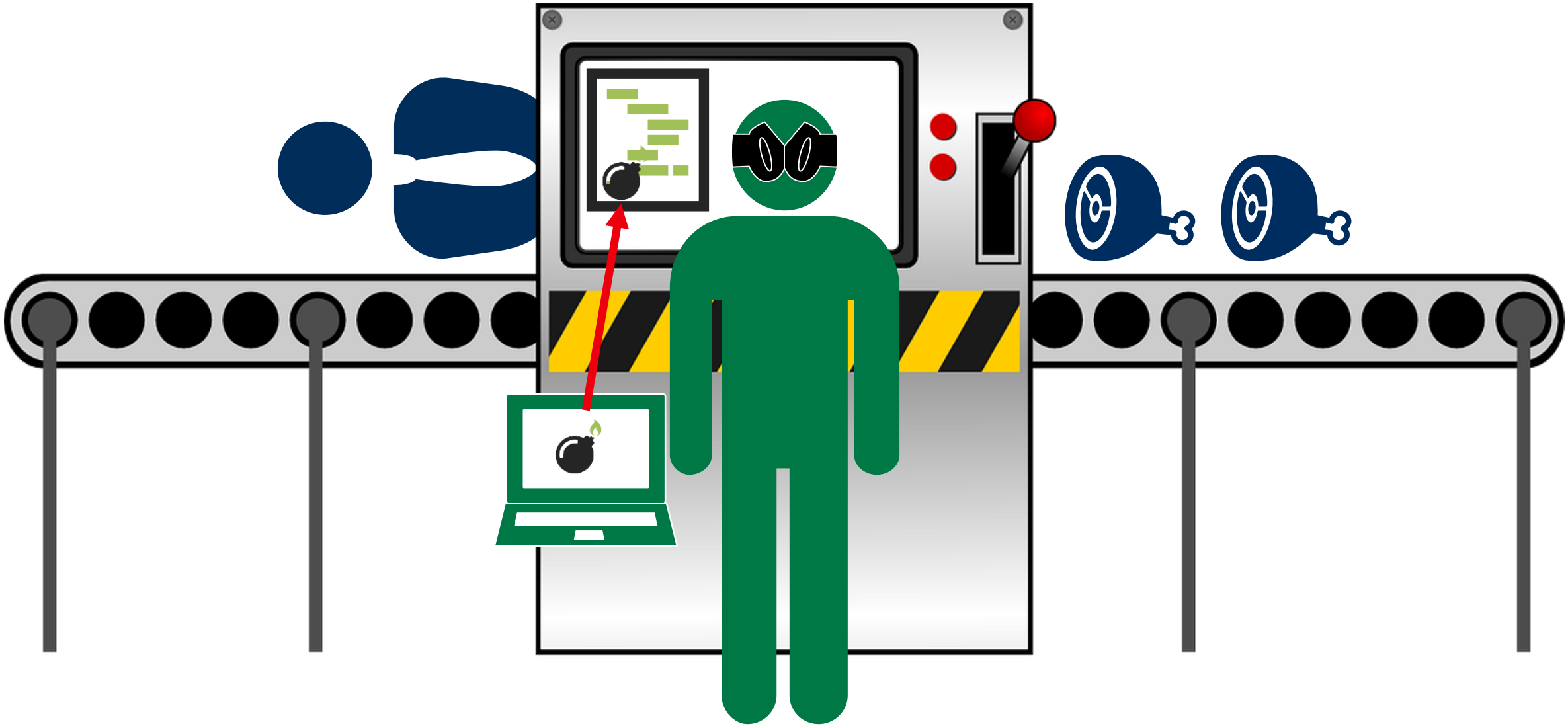
Safety und Security: Verknüpfung physischer und digitaler Systeme



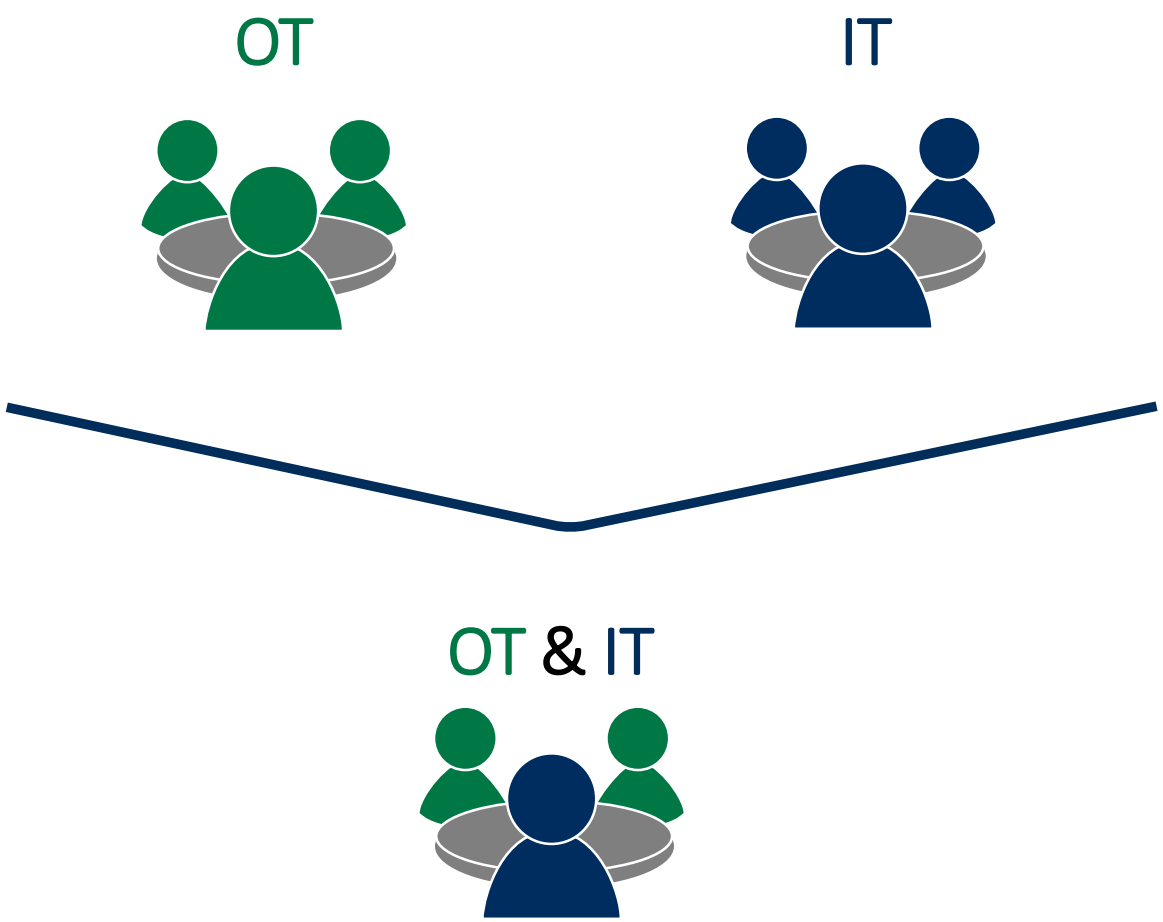
Safety vs Security - aus Sicht der Safety



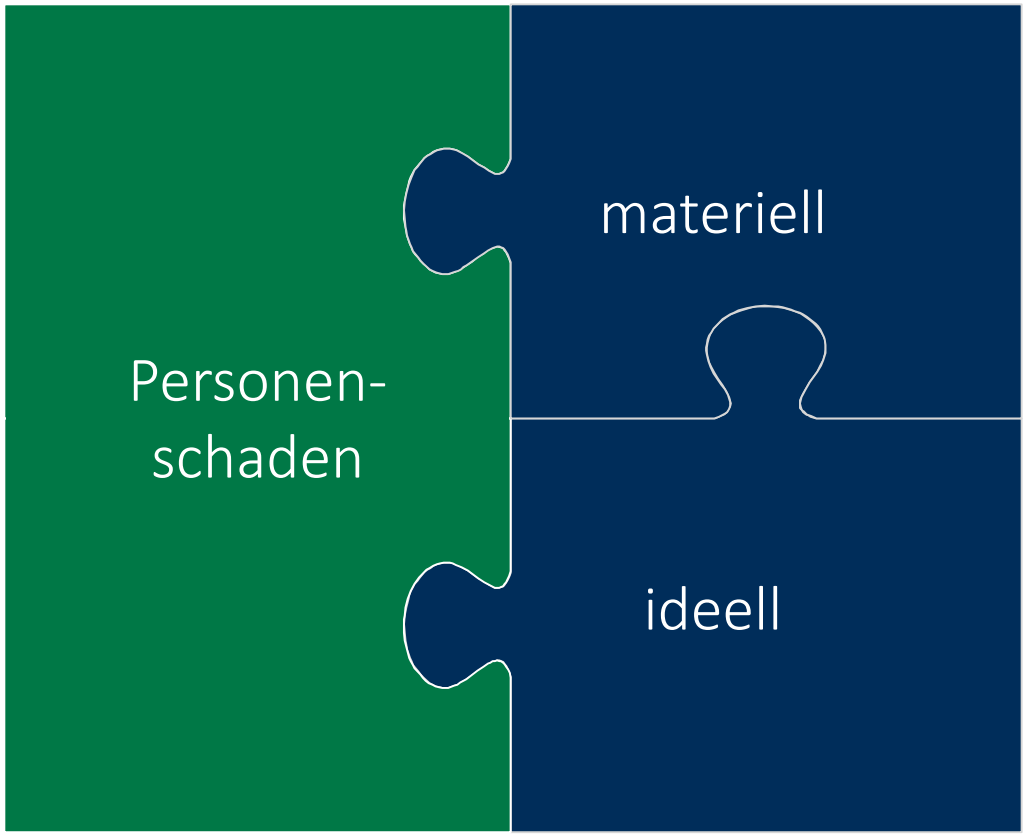
Safety vs Security - aus Sicht der Security



Mix Safety & Security

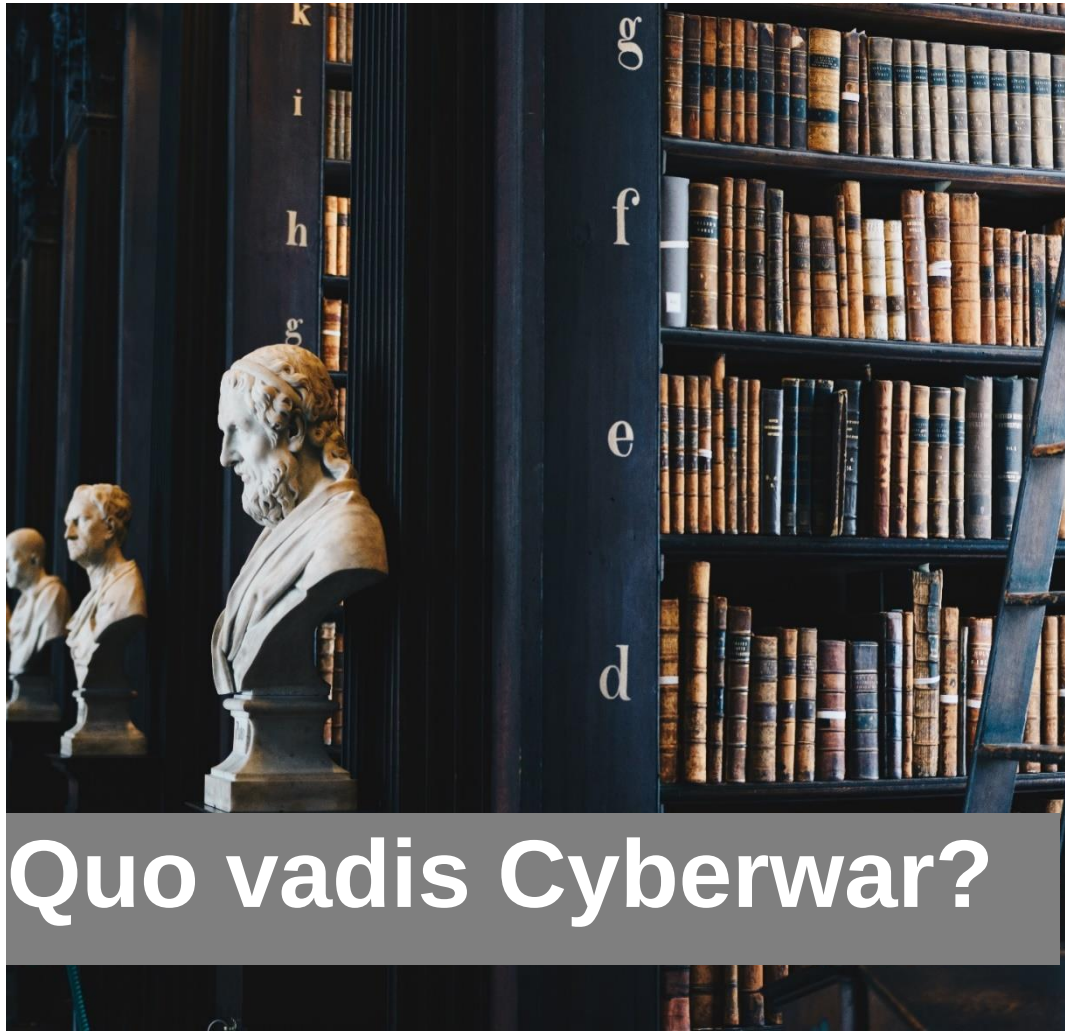


Schutzziele



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 <<

Krieg oder Zybervorfälle, Information Warfare & Hybride Bedrohungen?!?

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

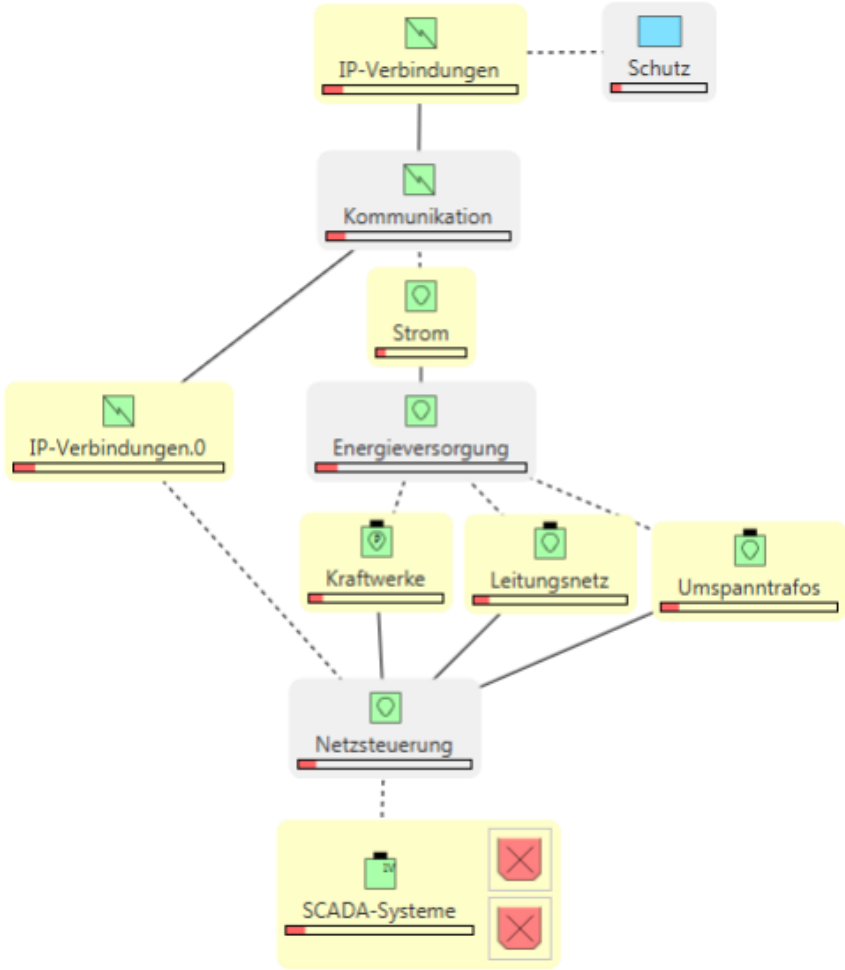
(durch militärischen Operationen „zur Aufklärung und Wirkung“)

- 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

militärische Cyber-Wirkketten

(Theorie)

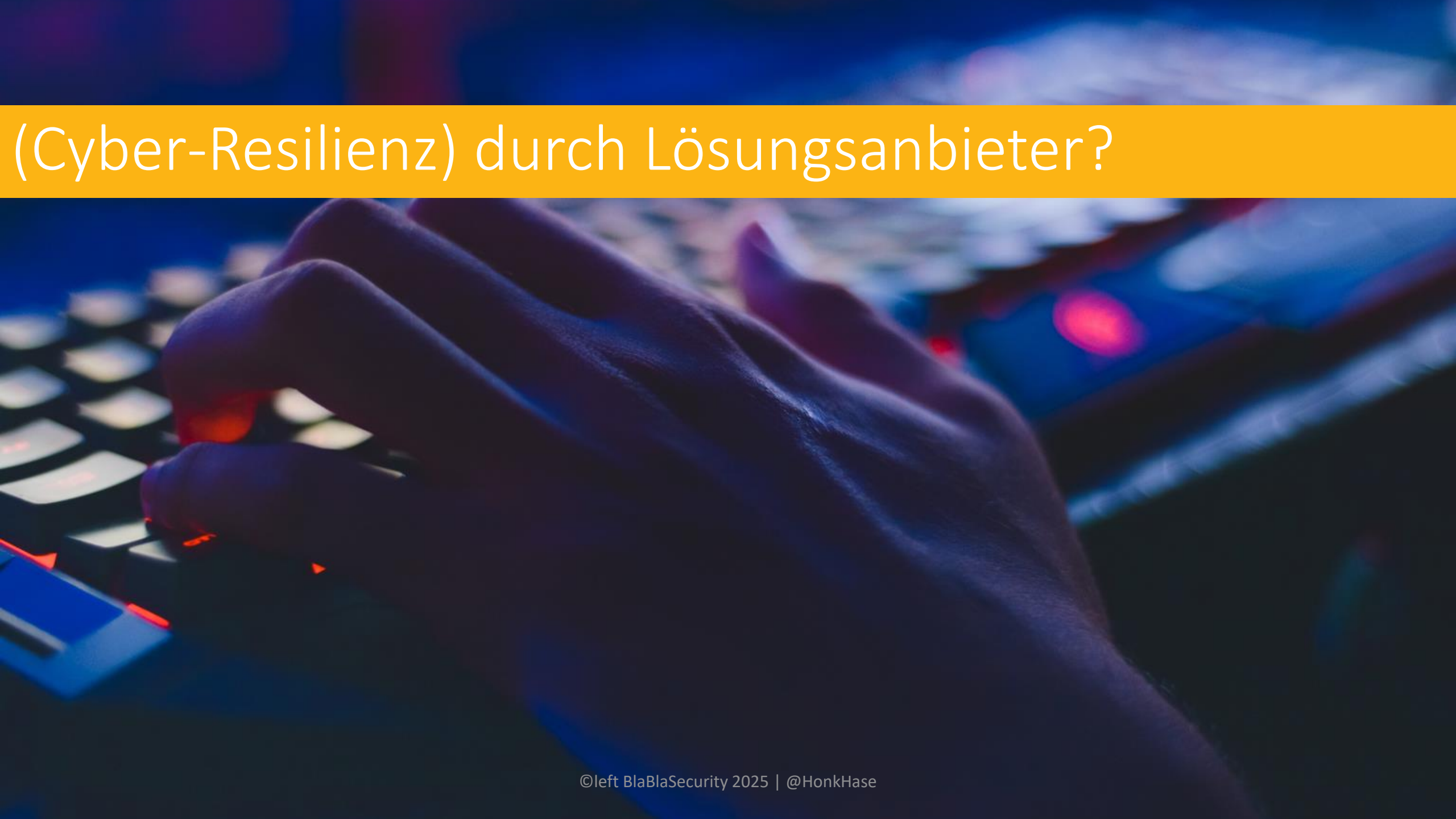
- **Cyberwirkung** löst häufig eine Kettenreaktion auf dem **Fähigkeits-Ressourcen-Netzwerk** aus
  - Angriff auf **SCADA-System** führt zum Ausfall der **Stromversorgung**
  - Ausfall der **Stromversorgung** führt zum Ausfall der **Telekommunikation**
  - Ausfall der **Telekommunikation** führt zum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



Cyberwar vs. Realität

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

(Cyber-Resilienz) durch Lösungsanbieter?



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

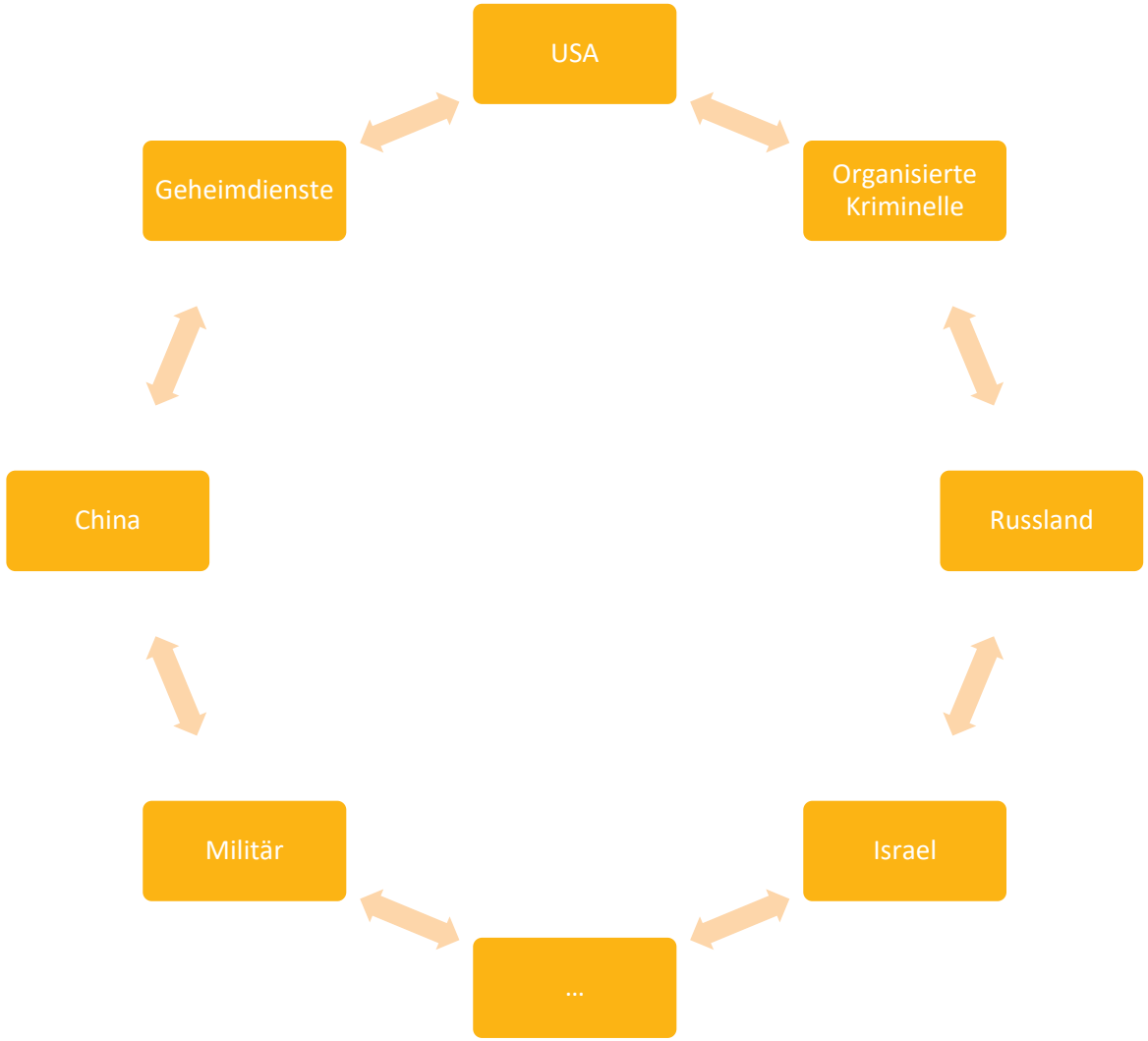
** Hallo, BSI Grundschutz (ISMS mit BCM)*

Bedrohungen und Gefährdungen

- Bedrohung
  Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann

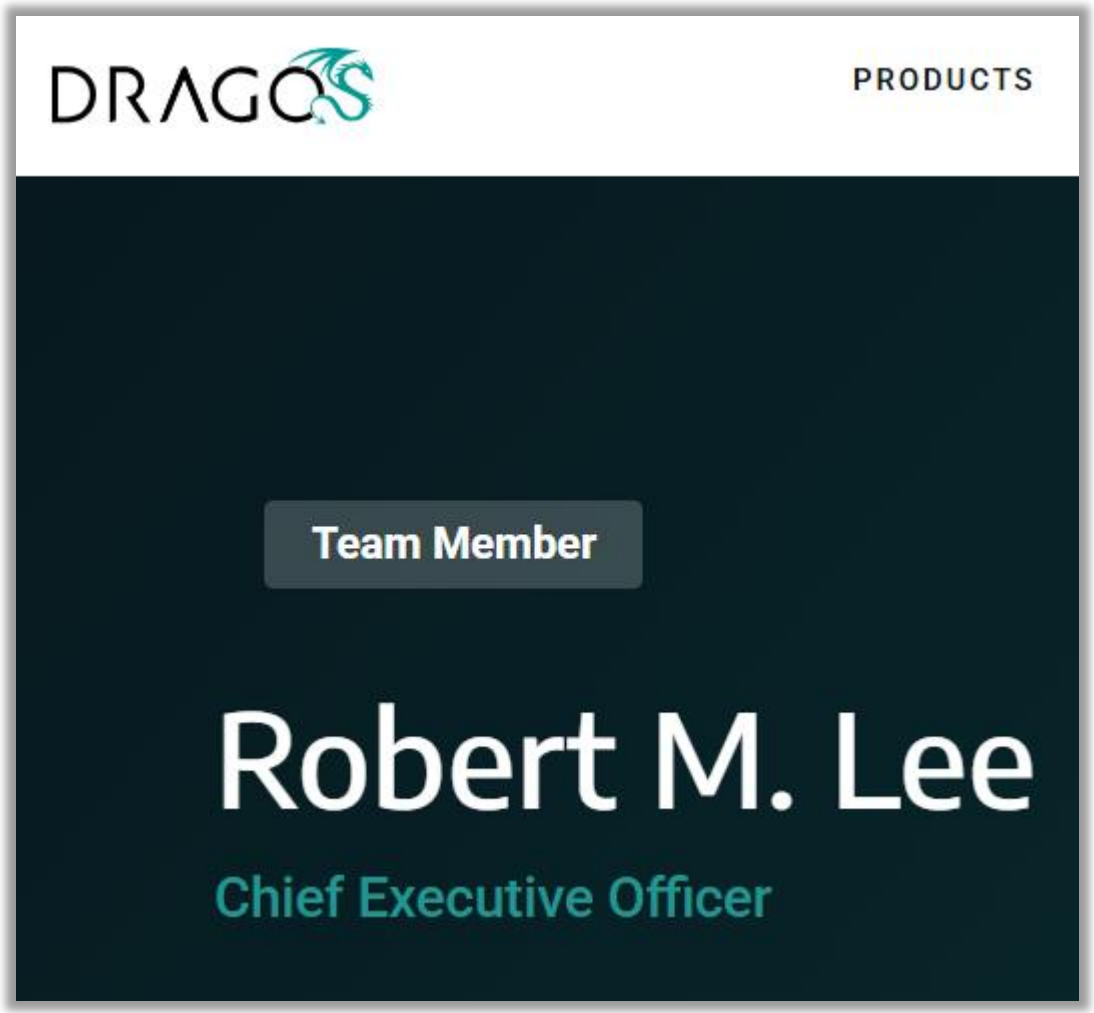
- Gefährdung
  Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.

Schutz vor was und wem?



Lieferkette: Crowdstrike

Lieferkette: Dragos



Robert began his pioneering work in ICS/OT cybersecurity as a U.S. Air Force Cyber Warfare Operations Officer tasked to the National Security Agency

Lieferkette: 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

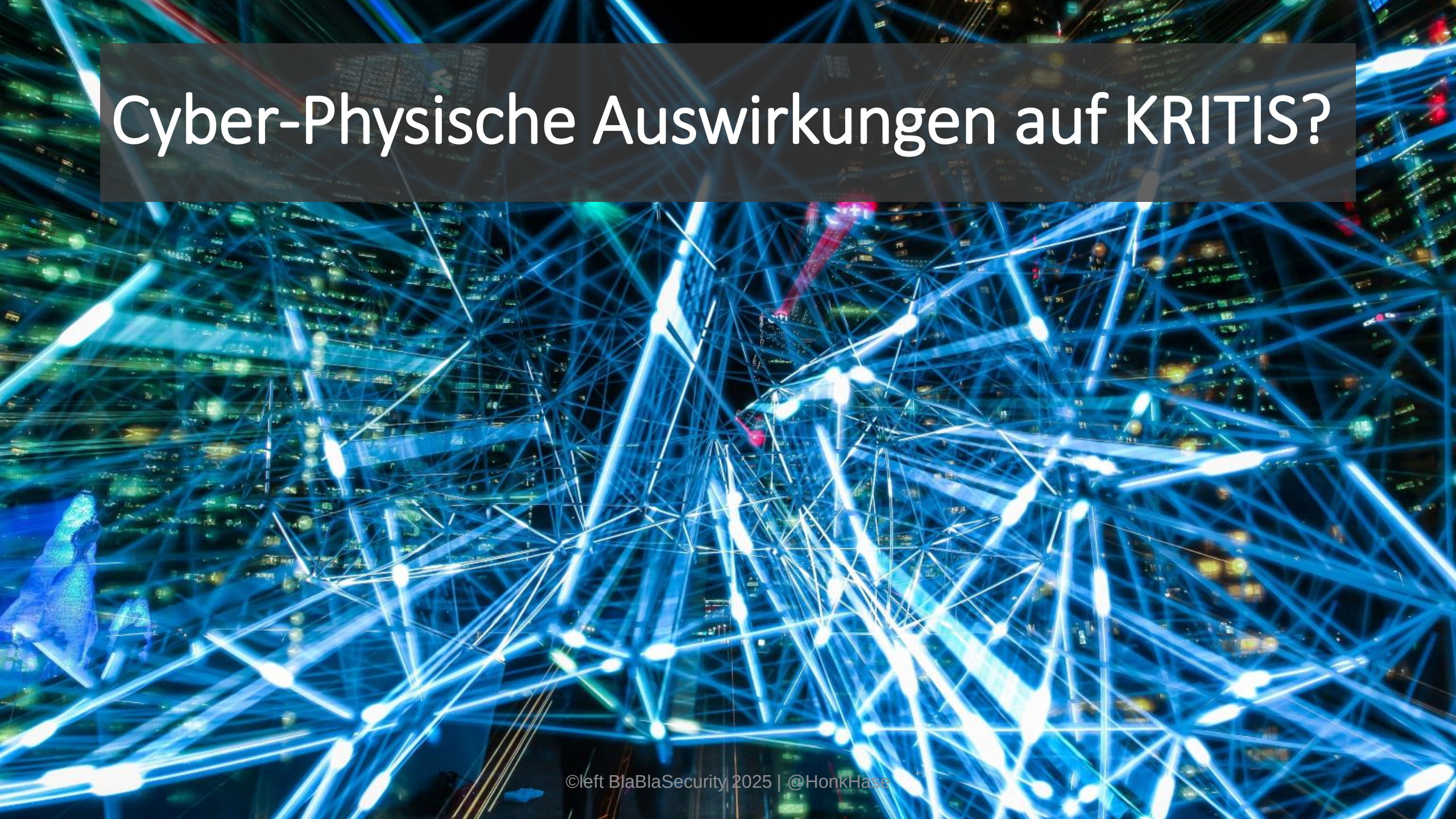
von Pierre Heumann

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, Versicherungsfirmen, Flughäfen, Energiefirmen, Regierungen, Logistikfirmen und Börsen zu seinen Kunden.

Cyber-Physische Auswirkungen auf KRITIS?



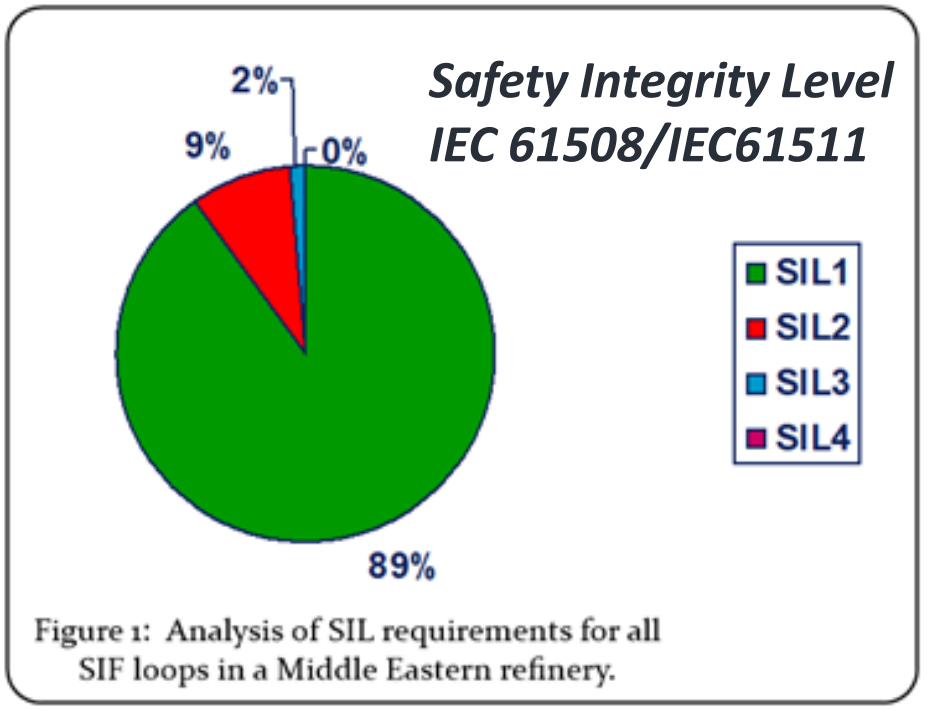


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.

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

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

>> 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