LÜKEX

BBK

Manuel ‚HonkHase‘ Atug

Hybride Kriegsführung im Cyberspace

Manuel ‚HonkHase‘ Atug

Manuel (HonkHase) Atug

Head of Business Development bei der HiSolutions AG

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- > 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

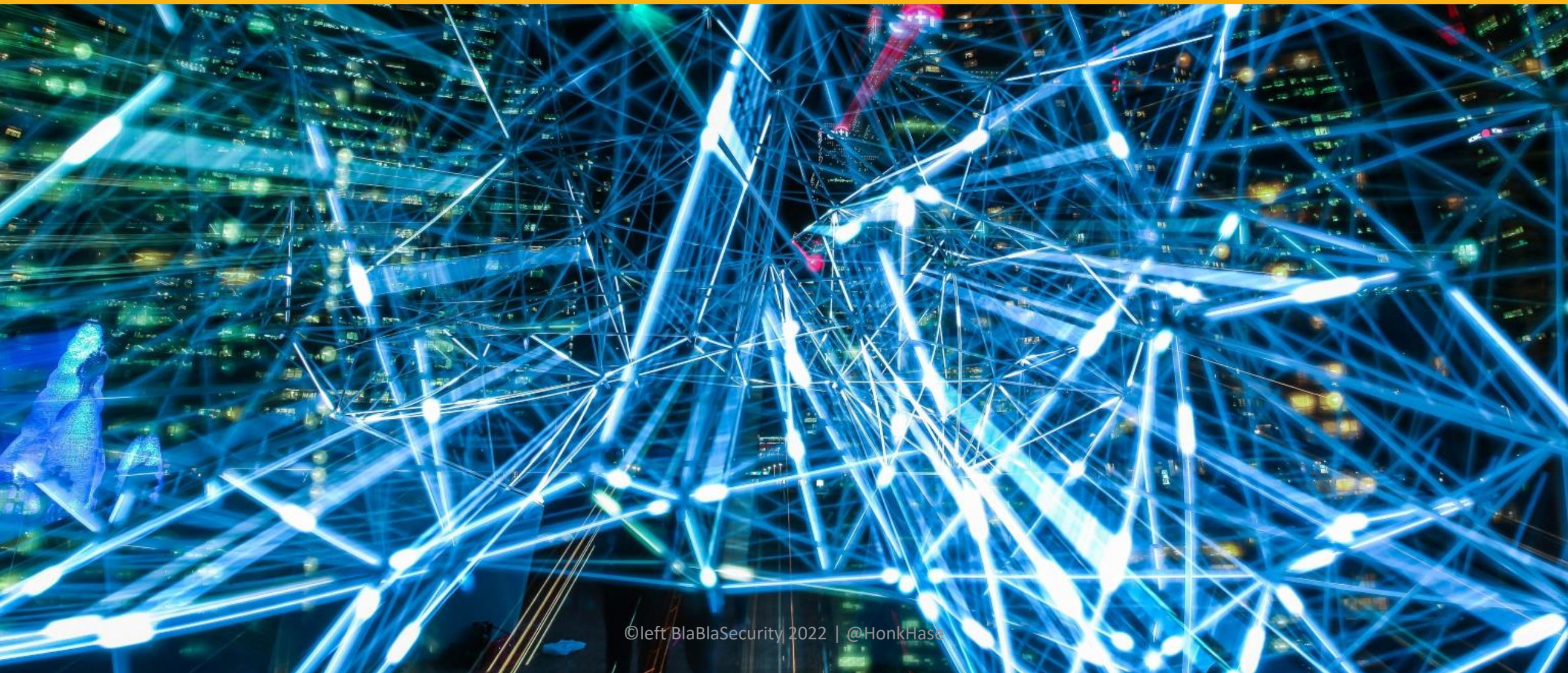
- Mitgründer der AG KRITIS: https://ag.kritis.info

- @HonkHase

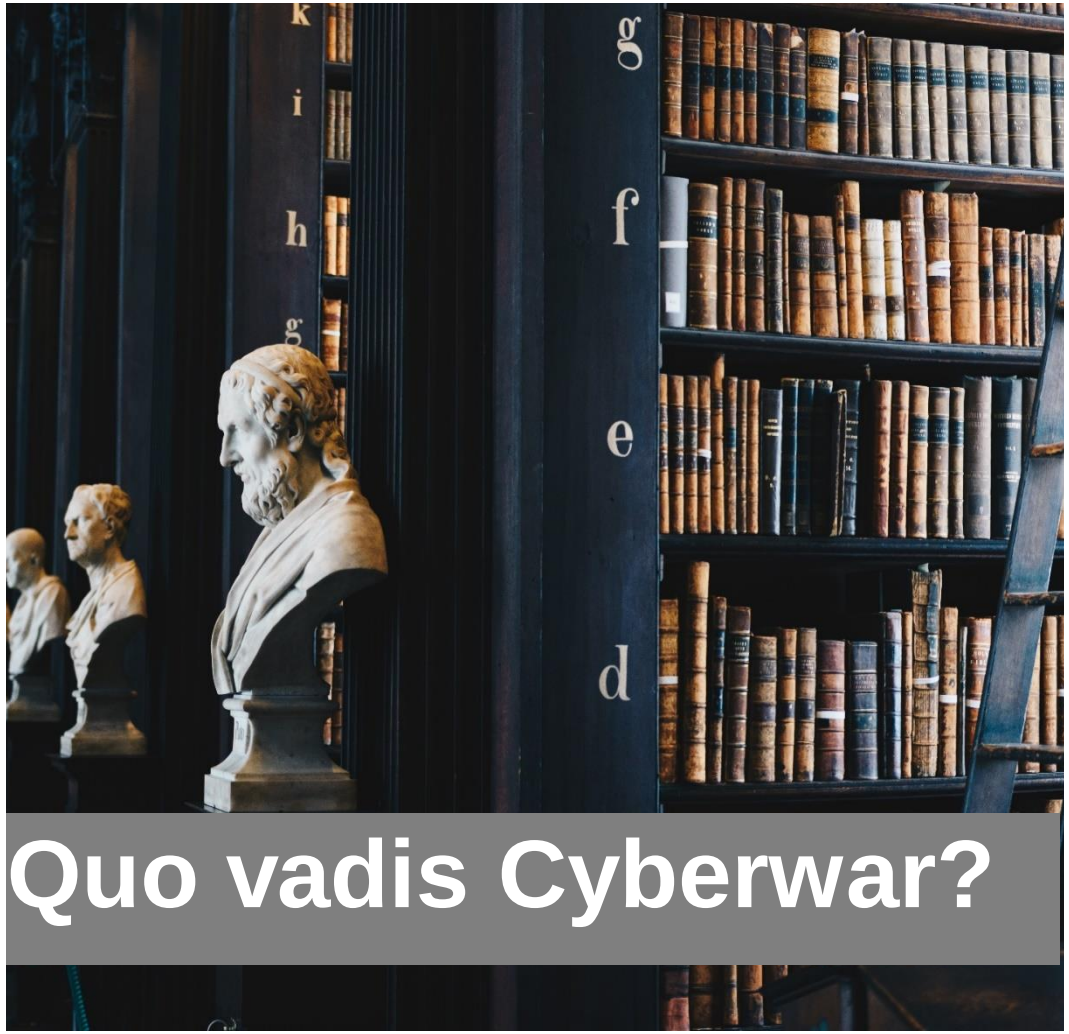
AG KRITIS

Ich habe #KRITIS im Endstadium

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

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

Cyberwehr

Wir. Dienen. Neuland.

Aber es ist doch Züberkrieg!

Cyberwar? Äh nö sorry!

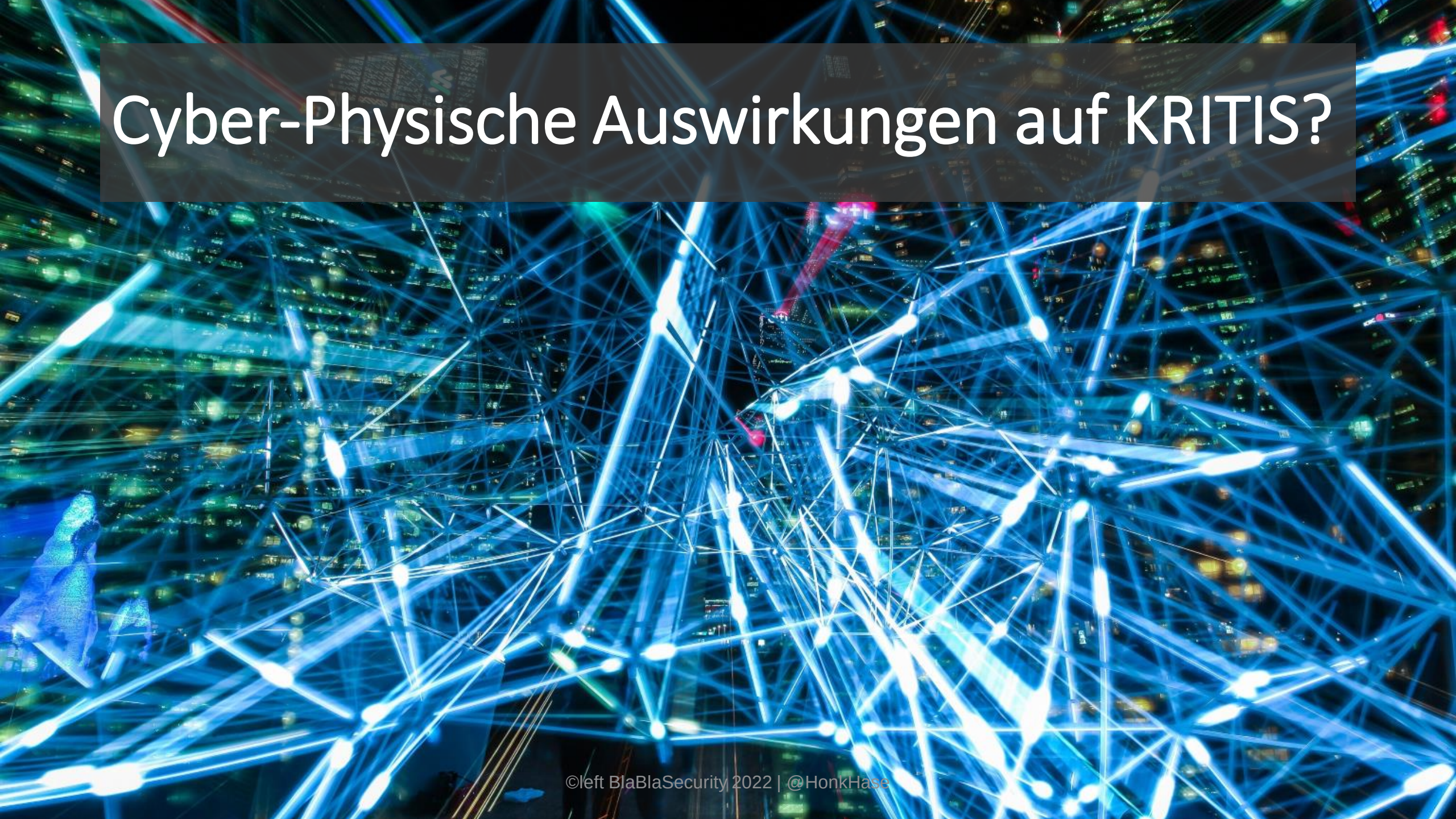
- Terabytes an Data Leaks russicher „Oligarchenfirmen“
- Conti Ransomware Group kooperiert mit dem FSB
  Best breed aus zwei Welten: Cybercrime & Geheimdienste
- Cyberwar vs Realität?
  - Cyberwar ist eher die bunte Powerpoint Foliengeschichte von Militärberatern, Rüstungsindustrie und zwielichtigen Securityproduktverkäufern
  - Realität ist ein permanentes Grundrauschen von Angriffen im Cyberraum
  - Dem einen Cyberraum für uns alle halt

©left BlaBlaSecurity 2022 | @HonkHase

Cyberwar vs. Realität

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

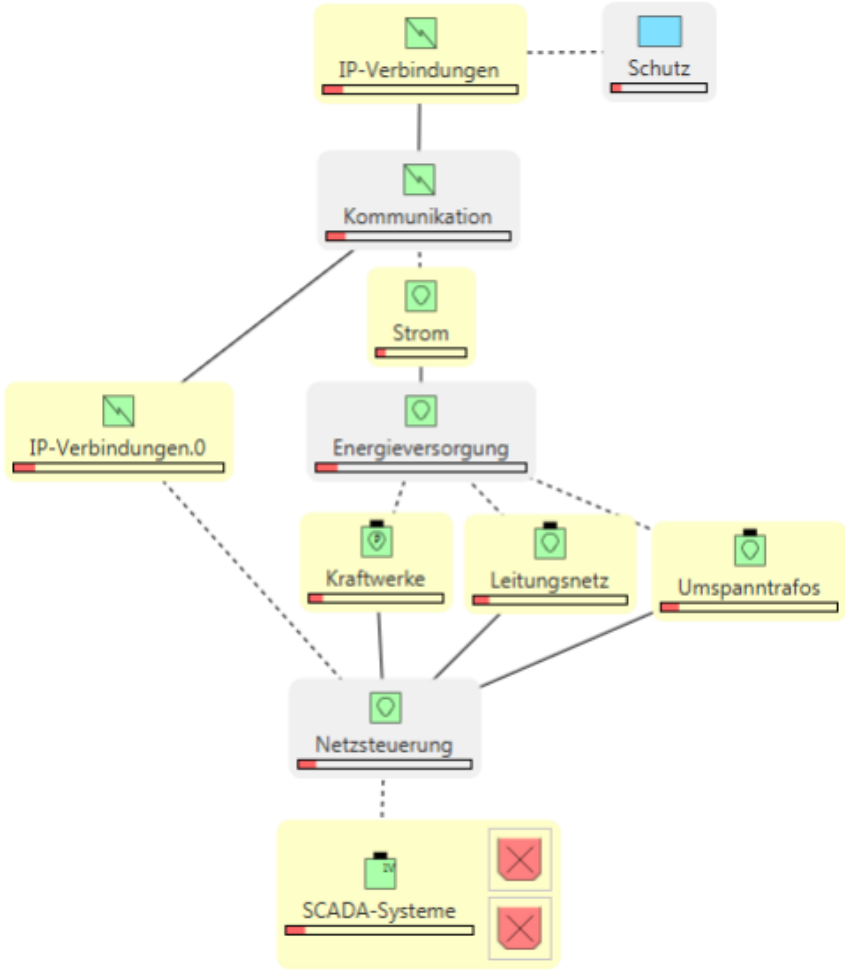
Cyber-Physische Auswirkungen auf KRITIS?



militärische Cyber-Wirkketten

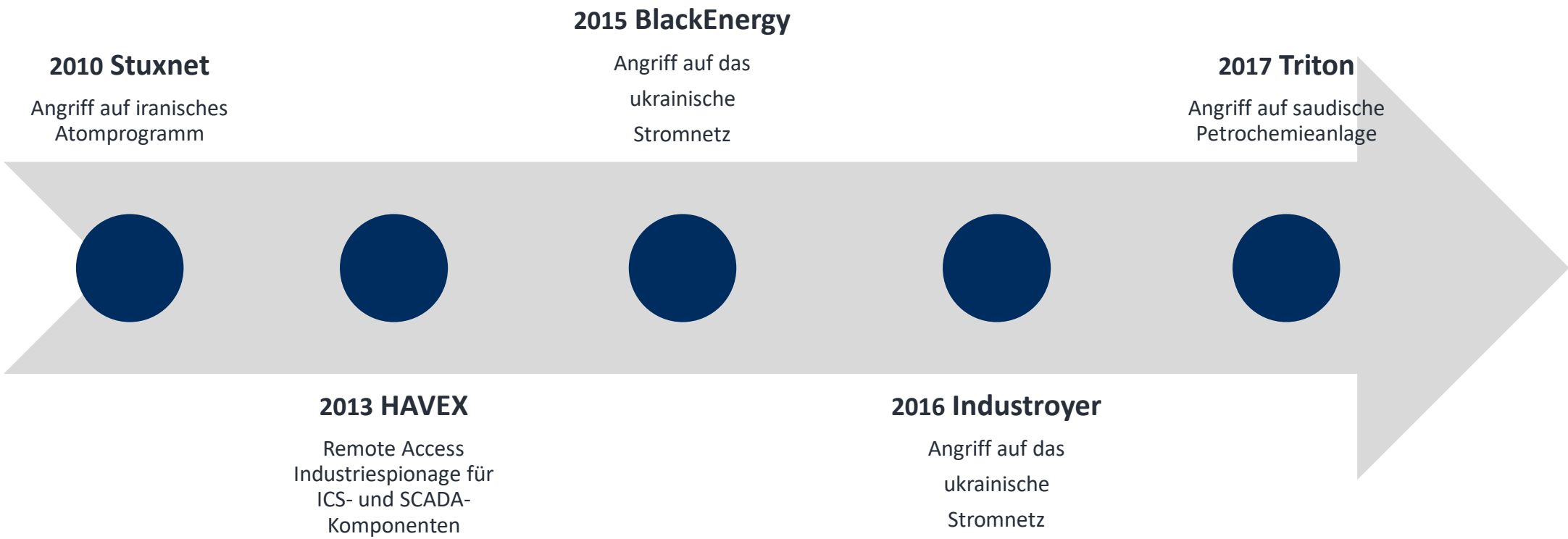
(Theorie)

- **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?)



Wie sehen also Cyber-typische Vorfälle im „Cyberwar“ aus?

- i.d.R. eher nicht langanhaltend, sondern temporär
- Wirtschaftliches Interesse
- Spionage und Aufklärung
- Fake News und Propaganda

- Umfassende Kollateralschäden möglich, aber in der Risikoanalyse nicht kalkulierbar

Gibt es denn Bedrohungen für KRITIS in Deutschland?

- Digitalisierung schreitet bei KRITIS (langsam) voran
- Ransomware wird mehr!
- Fachkräftemangel wird mehr!
- Naturkatastrophen werden mehr!

- Cyberwar- & 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*

Und was mache ich, wenn alles nichts hilft?

Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspflücker.de