BBK BABZ

Manuel ‚HonkHase‘ Atug

Multiple Krisen: Cybersicherheit

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: ag.kritis.info

AG KRITIS

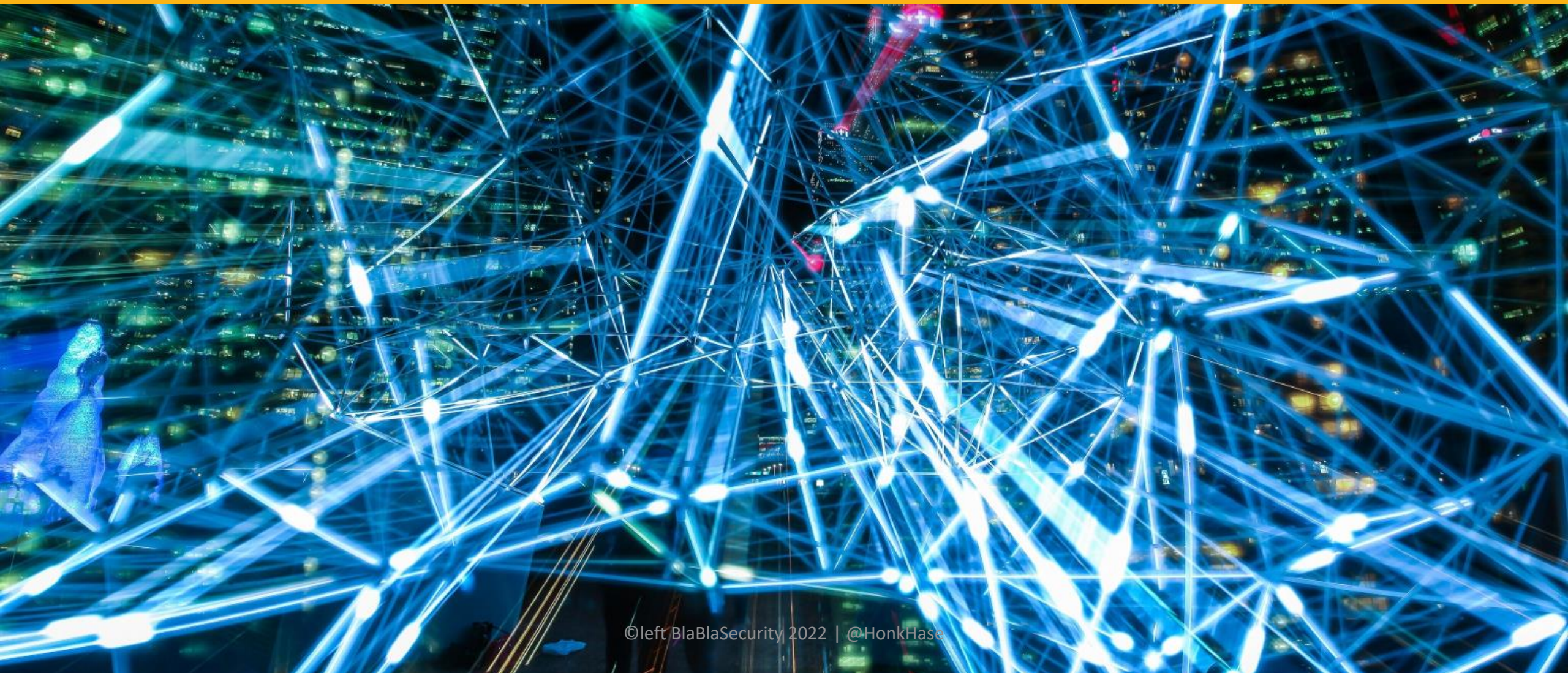
- Mitgründer der AGND: www.agnd.eu

AGND

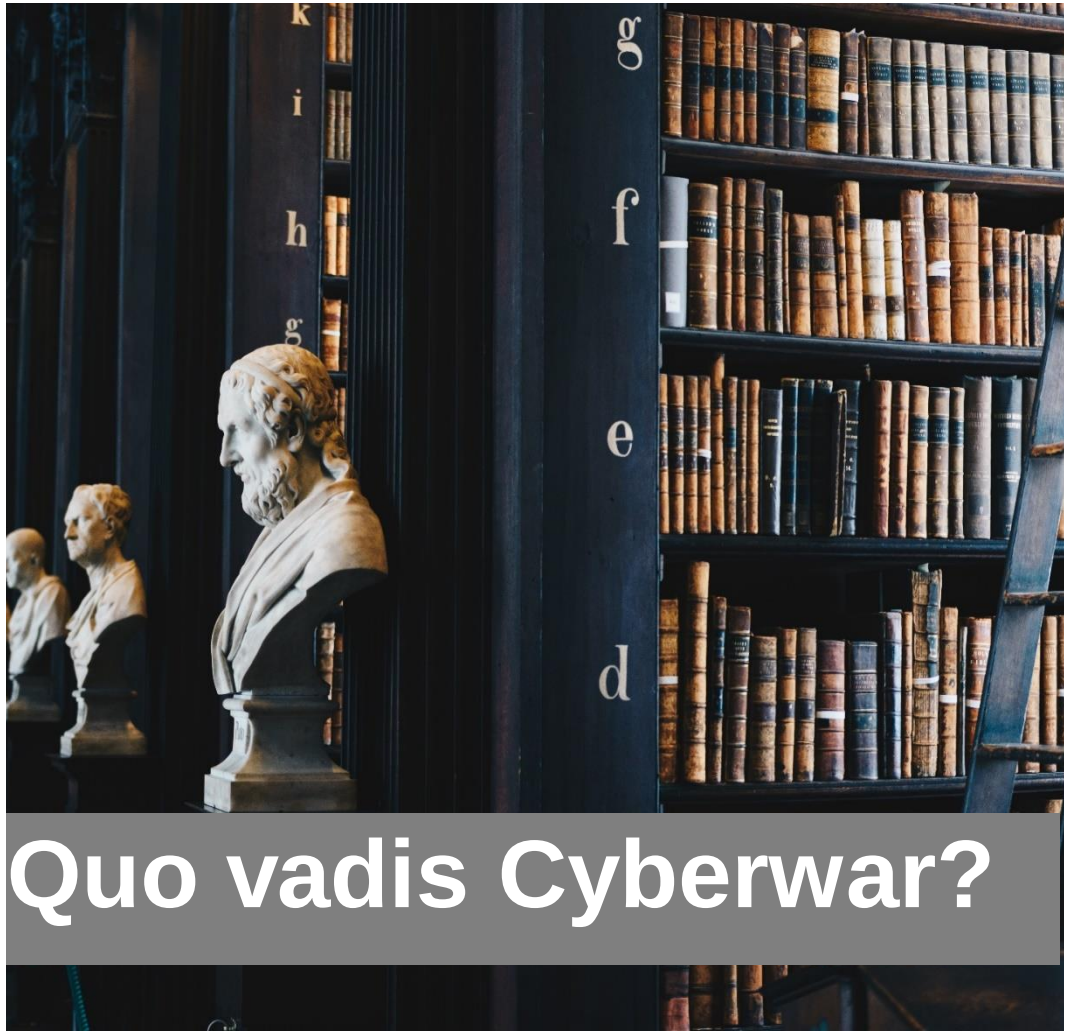
@HonkHase

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 <<

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)

Ziel militärischer Cyber-Operationen im Hybrid Warfare

(durch militärischen Operationen „zur Aufklärung und Wirkung“)

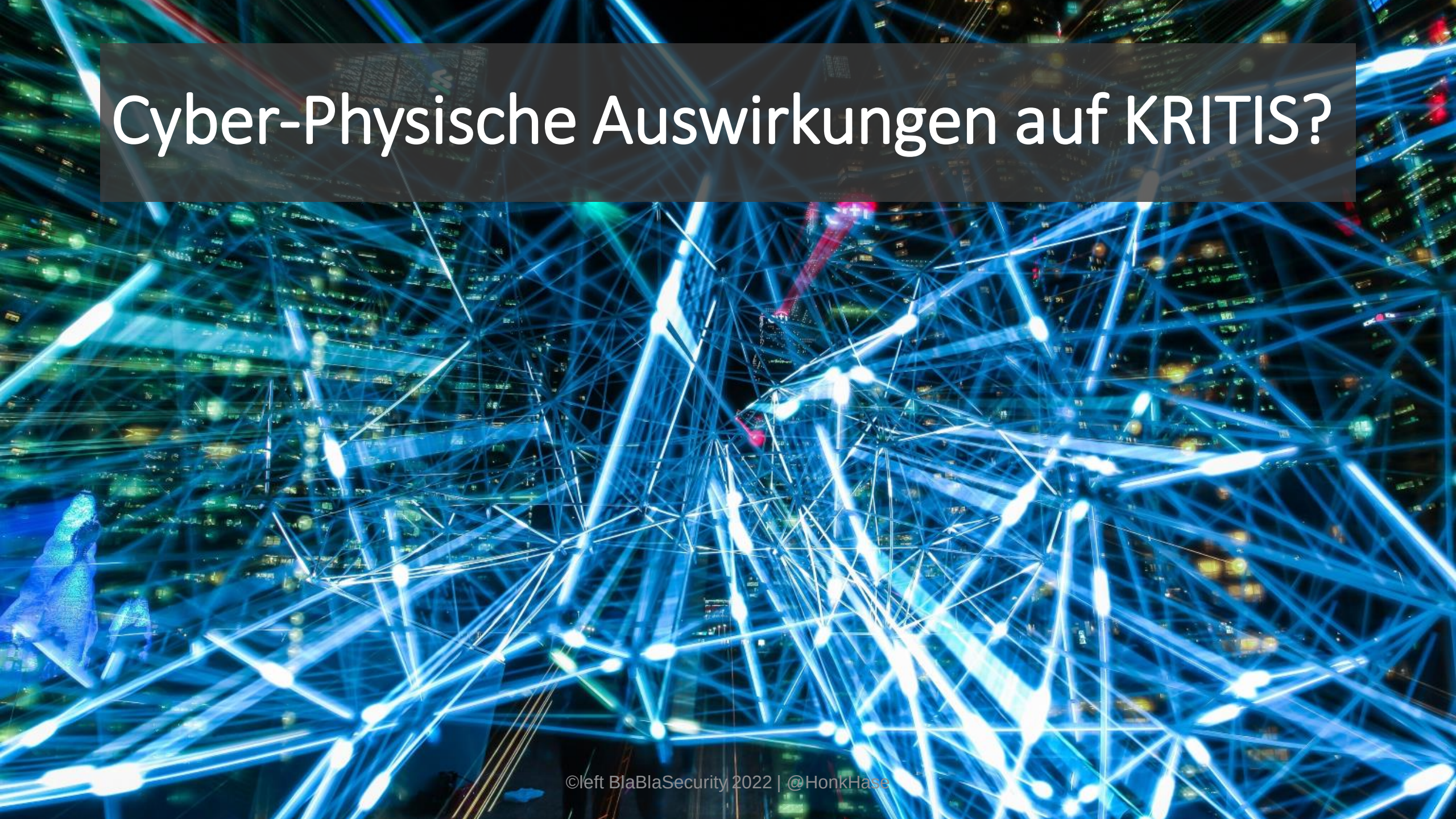
- Cyber-Operationen
  - Spionage
  - Beeinträchtigung der Führungsfähigkeit
  - Sabotage Kritischer Infrastrukturen (KRITIS)
  - Defacement von regierungseigenen Webseiten und offiziellen Kommunikationswegen
  - Desinformation über soziale Medien
  - Blockade des nationalen Zugangs zum Internet

KRITIS in Putins Angriffskrieg gegen Ukraine

Cyberwar vs. Realität

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

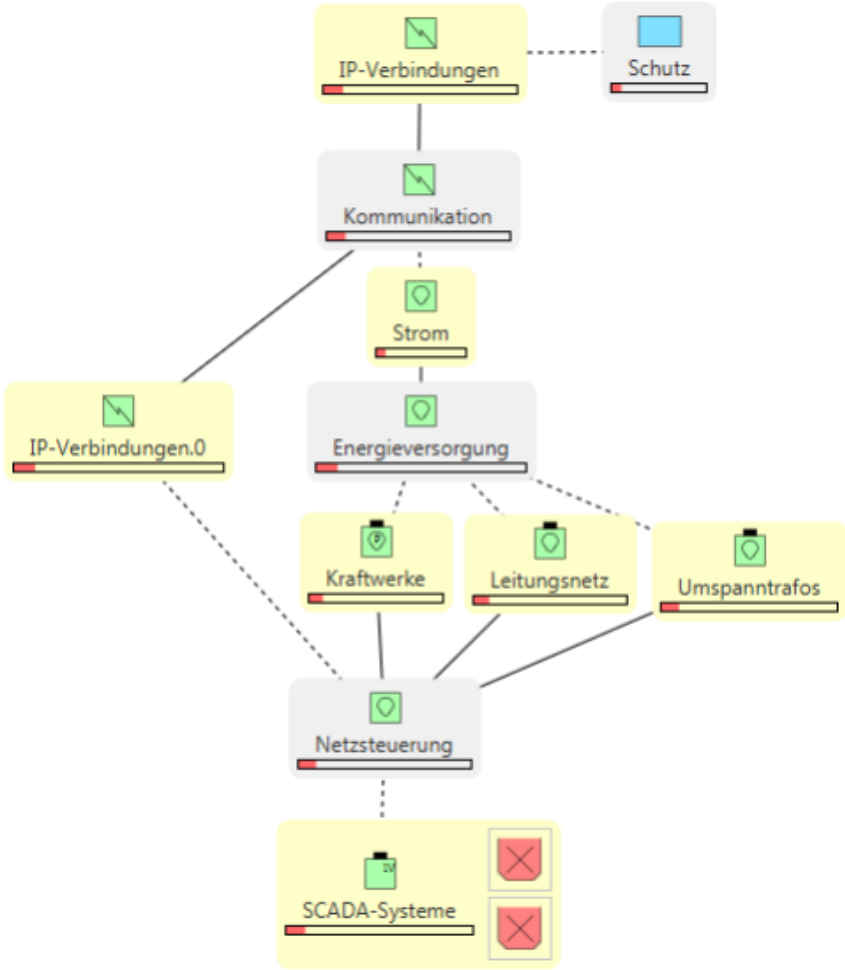
Cyber-Physische Auswirkungen auf KRITIS?



militärische Cyber-Wirkketten

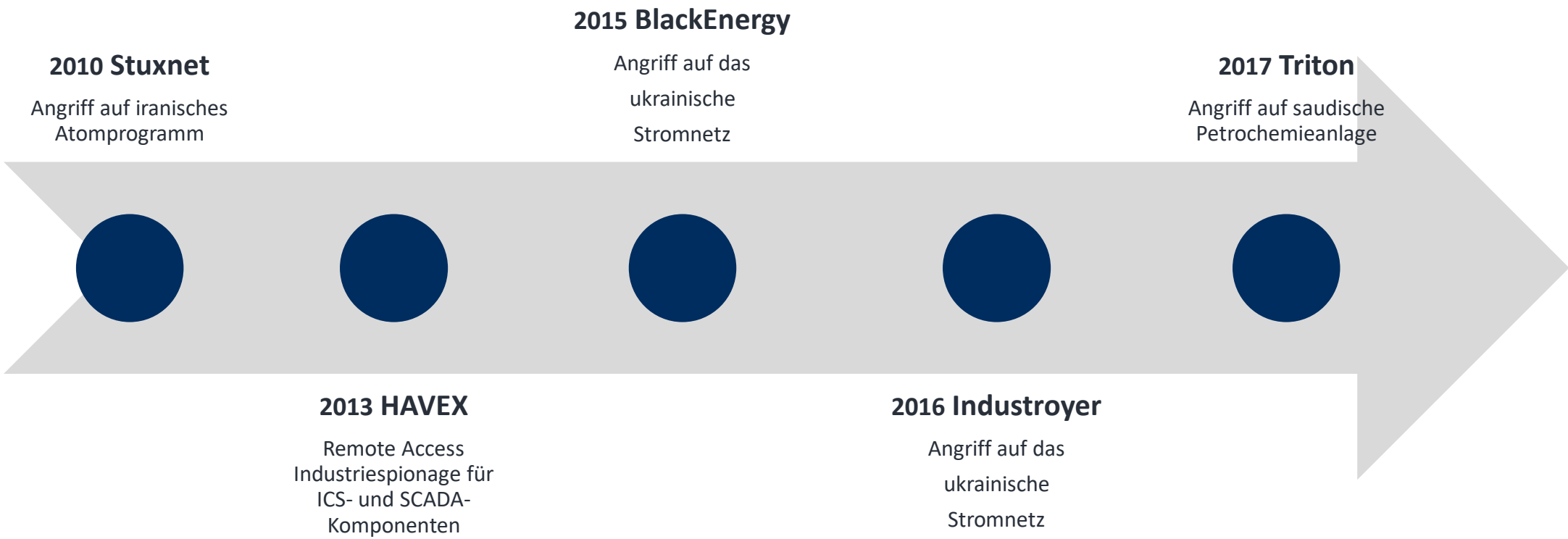
(Theorie)

- **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 (zB Ransomware)
- Spionage und Aufklärung
- Fake News und Propaganda

- Umfassende Kollateralschäden möglich, aber in der Risikoanalyse nicht kalkulierbar

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

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*

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? (ID Wallet, Luca App)

  →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!

- Vermeiden sie daher technische Schulden an kommende Generationen

- 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