

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 lighting is dramatic, with strong shadows and highlights on the metallic surfaces.

MIV Arbeitskreis IT-Sicherheit

Manuel „HonkHase“ Atug

A complex industrial piping system made of stainless steel. It features numerous horizontal and vertical pipes, valves, and flanges. Several yellow triangular warning labels with wavy lines are attached to the pipes. Two prominent blue and white electronic flow meters are mounted on the pipes, with red and purple cables connected to them. Several circular pressure gauges with white faces and black markings are also visible. The background shows more industrial equipment and a metal safety cage.

Aktueller Stand der IT-Sicherheitslage in Deutschland

Manuel „HonkHase“ Atug

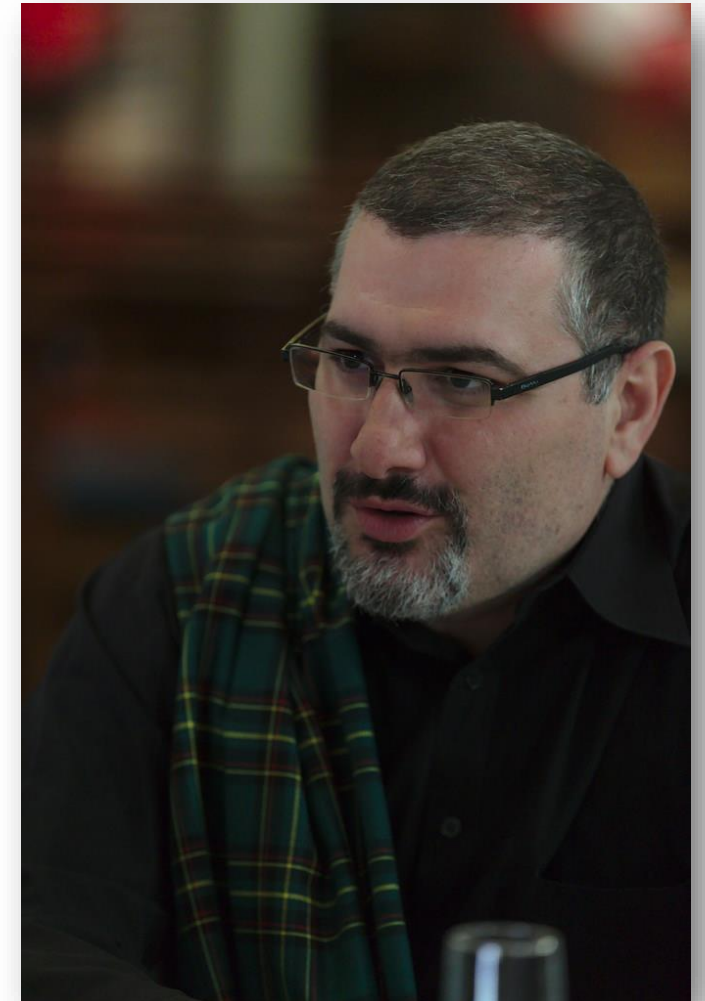
Manuel (HonkHase) Atug

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](https://twitter.com/HonkHase)



Ich habe #KRITIS im Endstadium



Was sind KRITISche Infrastrukturen?



Die 10 Kritische Infrastruktur Sektoren in Deutschland

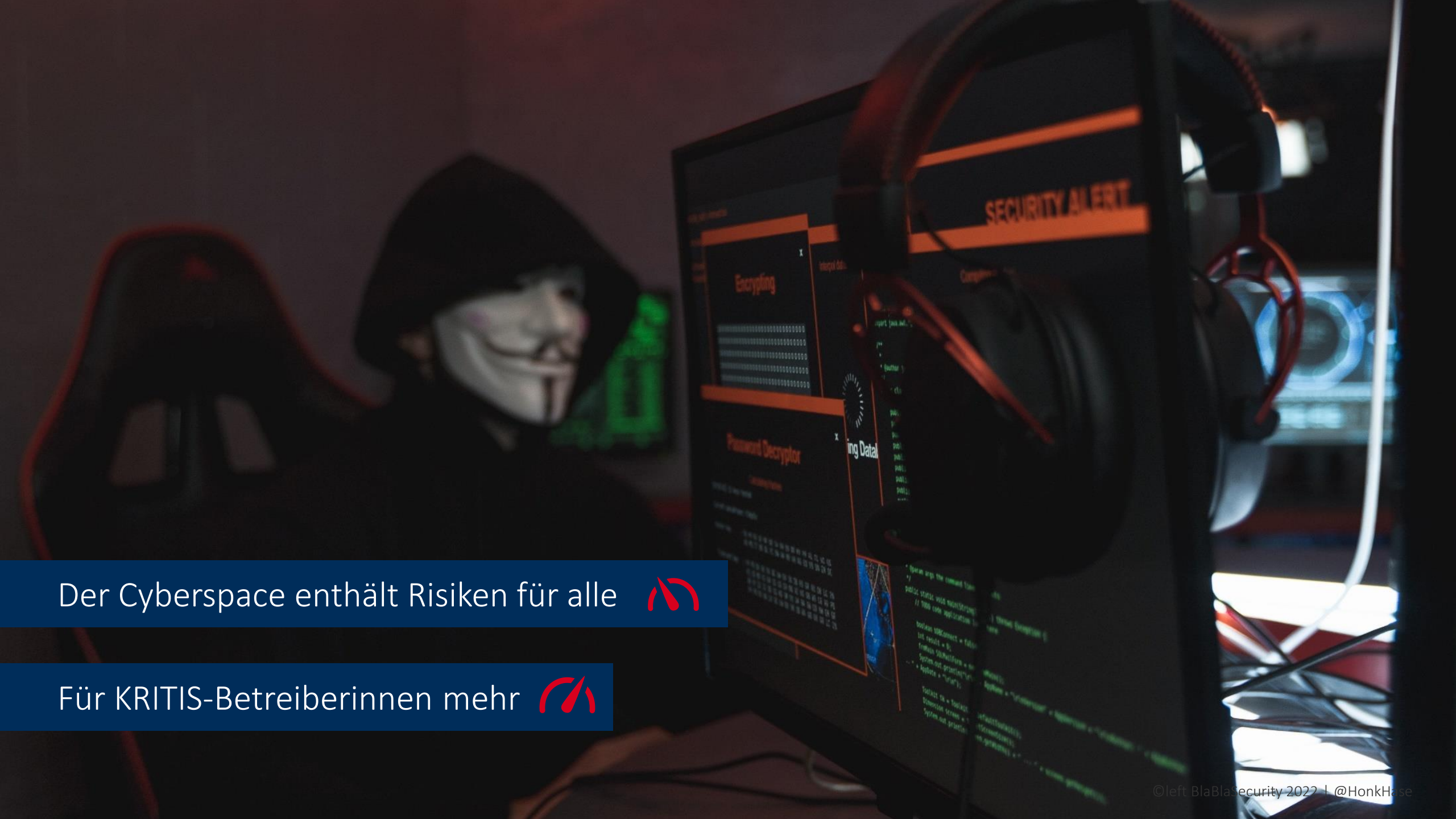


Quelle https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html



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!**



Der Cyberspace enthält Risiken für alle

Für KRITIS-Betreiberinnen mehr

The background of the slide is a complex, abstract digital network. It features a dense web of glowing blue lines and nodes, resembling a fiber-optic network or a data visualization of a large-scale system. The lines vary in thickness and brightness, creating a sense of depth and movement. In the upper left, there are some blurred, colorful shapes that look like data packets or light trails. The overall color palette is dominated by blues and whites, with some hints of green and red in the background.

Gibt es einen Cyberwar? Was ist das?

Zyberkrieg?



Quo vadis Cyberwar?

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

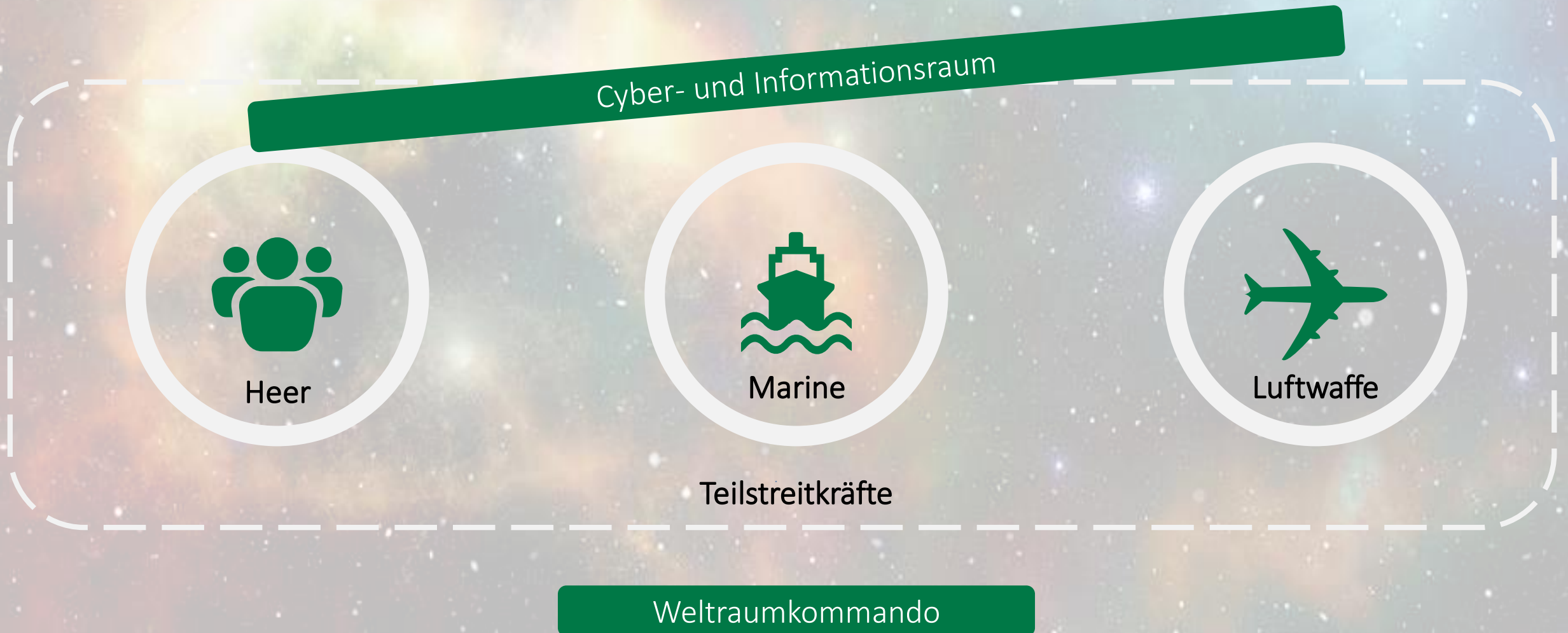
Zybervorfälle, Information Warfare & Hybrid Warfare!



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



Aber es ist doch Züberkrieg!

Cyberwar? Äh nö sorry!

- Terabytes an Data Leaks russischer „Oligarchenfirmer“
- 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





Cyberwar vs. Realität

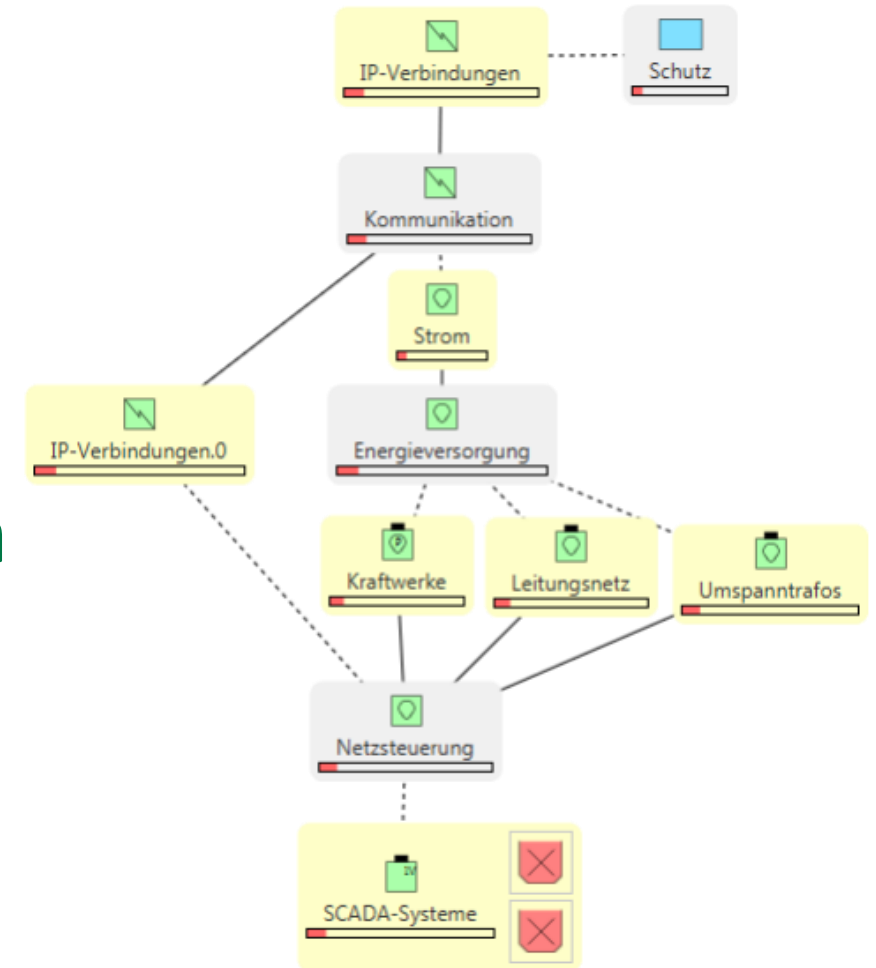
**Der Cyberwar findet auf PowerPoint-Folien statt,
in der Realität ist es ein Krieg der Bomben und Granaten**

Cyber-Physische Auswirkungen auf KRITIS?

militärische Cyber-Wirkketten

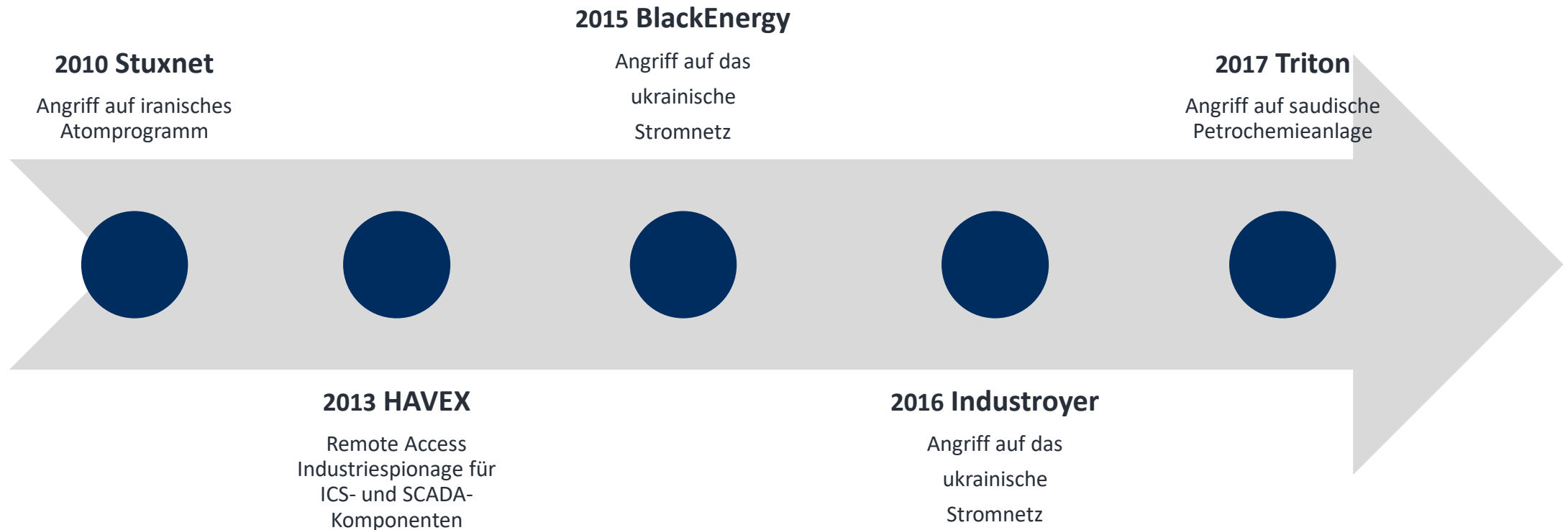
(Theorie)

- **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?)



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

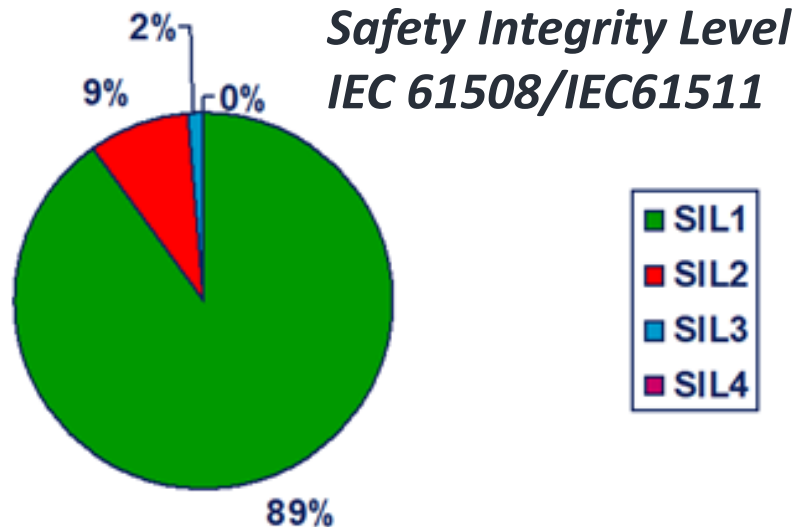


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.



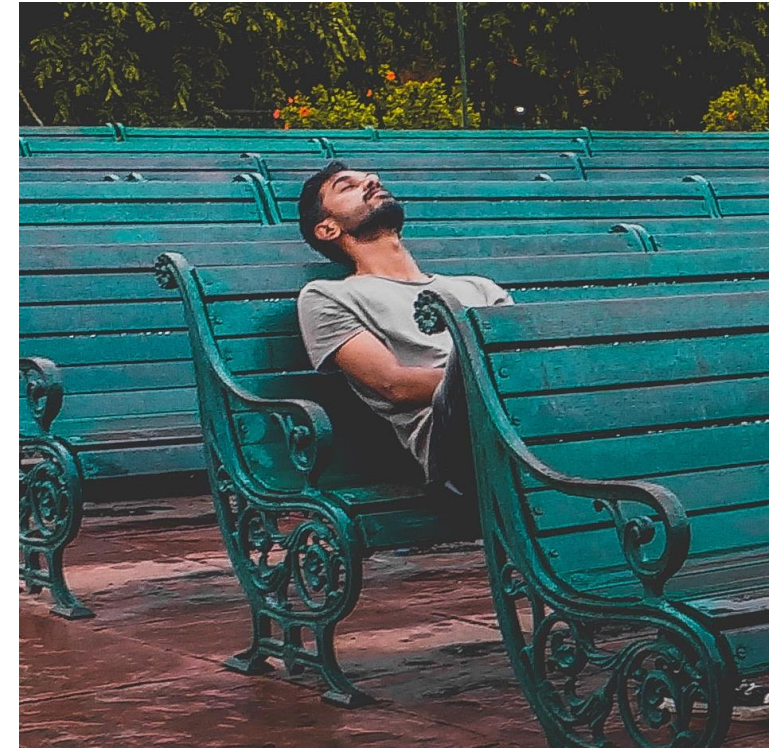
Safety-PLC gemäß Safety Instrumented System (SIL3)
Firmware wurde im RAM gezielt manipuliert

Attacke auf Saudi Arabisches Petrochemiewerk

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

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



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

Gibt es denn Bedrohungen für KRITIS?

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

Cyber-Verteidigung

(...die langweiligen Basics der IT-Security)

Büroalltag in der Defense

Haben wir ein Backup?

Ist es frisch oder fermentiert es vor sich hin?

Haben wir das sogar Offline vorliegen?

Haben wir mal die Wiederherstellung getestet?

Braucht das Wiedereinspielen viel zu lang?

Firewall? Same!

Nutzerverwaltung? Same! ...



>> 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

