

A black and white photograph of an industrial facility, likely a steel mill or refinery. The image shows a complex network of large pipes, metal walkways, and structural steel. In the foreground, a large, dark, curved pipe dominates the left side. The background features a tall, multi-story industrial structure with various pipes and platforms. The overall scene is industrial and technical.

# GUUG 2019

Linuxhotel Essen

Manuel (HonkHase) Atug





# Verantwortung und Ethik im Umfeld der KRITISchen Infrastrukturen

Manuel (HonkHase) Atug



Ich habe #KRITIS im Endstadium

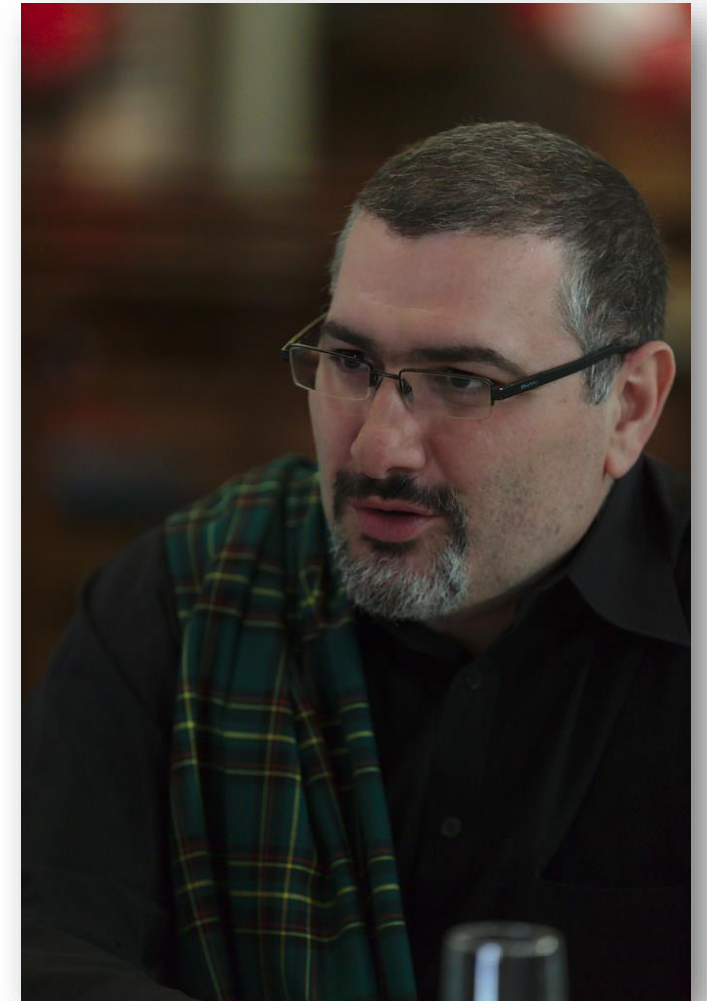
# Manuel (HonkHase) Atug

Senior Manager bei der HiSolutions AG

- Diplom-Informatiker & Master of Science in Applied IT Security
- > 23 Jahren in der Informationssicherheit tätig
- Prägender Berater des BSI für § 8a BSIg
- Meine Themen: KRITIS, Hackback, hybrid Warfare, Ethik

Seit ~23 Jahren Aktiv in so n paar Vereinen:

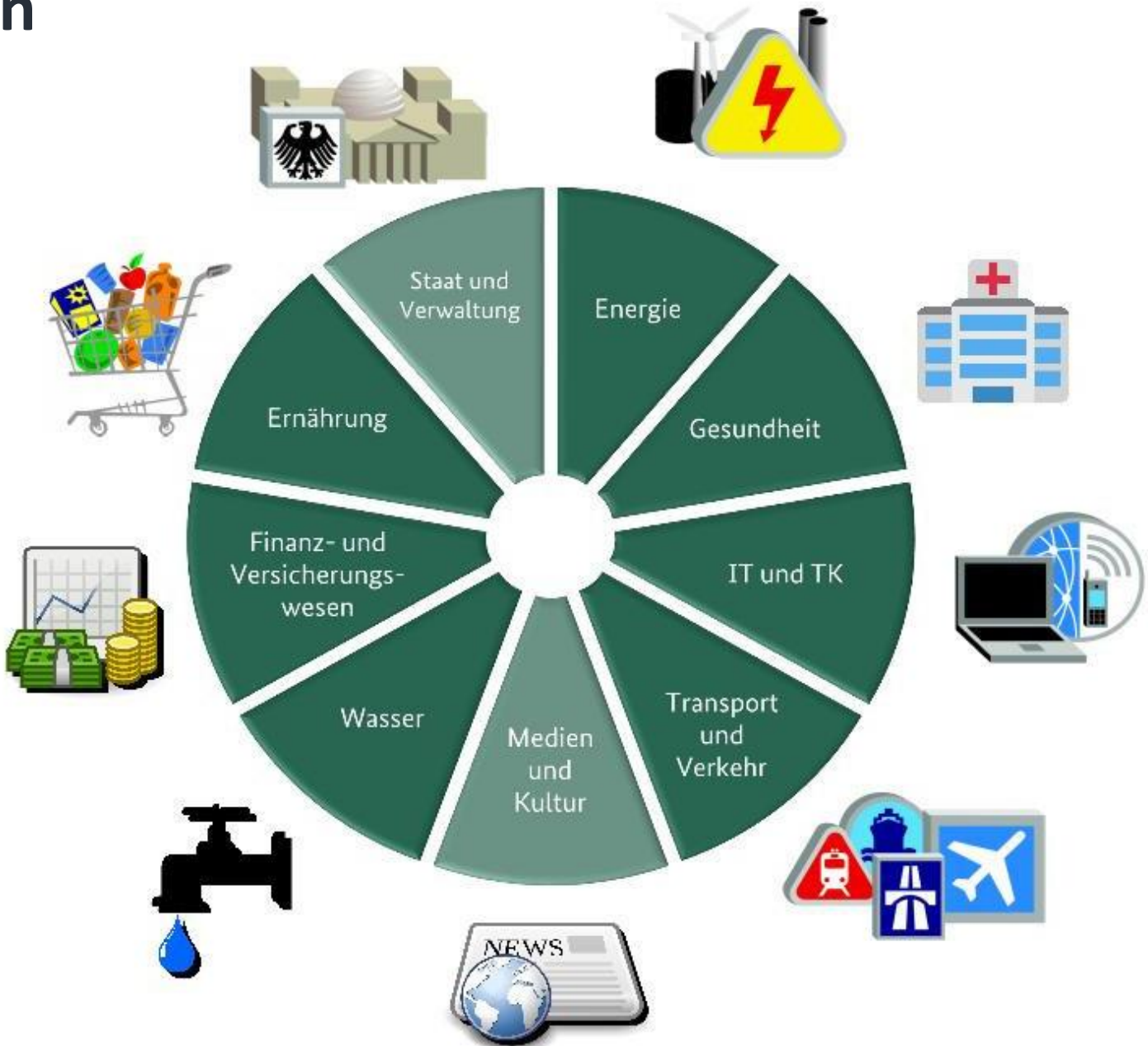
- Chaos Computer Club e.V., Chaos Computer Club Cologne e.V., c-base e.V., Digitale Kultur e.V., ISACA, GI e.V., FIF e.V., Cyber Security Cluster Bonn e.V., Freie Software Freunde e.V., Geraffel Core Member
- Leitung der AG KRITIS: <https://ag.kritis.info>
-  [@HonkHase](https://twitter.com/HonkHase)



# Was sind KRITISche Infrastrukturen?



# KRITIS Sektoren





# Kritische Dienstleistungen

Sprach- und Datenübertragung

Versicherungsdienstleistungen

Stromversorgung Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten

Lebensmittelversorgung

Kartengestützter Zahlungsverkehr

Personen- und Güterverkehr

Trinkwasserversorgung

Fernwärmeversorgung

Bargeldversorgung

Abwasserbeseitigung

Laboratoriumsdiagnostik

Konventioneller Zahlungsverkehr

stationäre medizinische Versorgung

Gasversorgung

Verrechnung und Abwicklung von Wertpapier- und Derivatgeschäften

Kraftstoff- und Heizölversorgung

Datenspeicherung und -verarbeitung

Versorgung mit verschreibungspflichtigen Arzneimitteln

# Schutz Kritischer Infrastrukturen (Schutzbedürfnis)





## 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!**



# Was ist Ethik (vs. Moral)?



# Begriffsbestimmung

## Moral

- Gesamtheit von ethisch-sittlichen Normen, Grundsätzen, Werten, die das zwischenmenschliche Verhalten einer Gesellschaft regulieren, die von ihr als verbindlich akzeptiert werden
- "die öffentliche Moral"

## Ethik

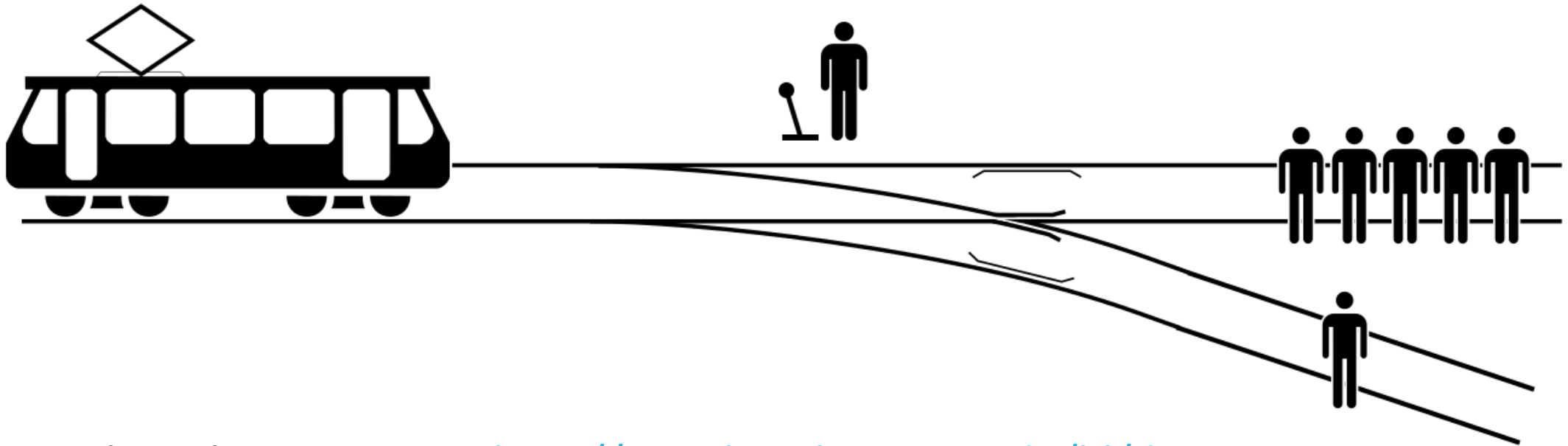
- Gesamtheit sittlicher Normen und Maximen, die einer [verantwortungsbewussten] Einstellung zugrunde liegen
- "sein Handeln war von christlicher Ethik geleitet"



# Trolley-Problem (Weichenstellerfall)

## Moralisches Gedankenexperiment

- Kann beliebig verkompliziert werden
- Es gibt kein „richtig“ oder „falsch“... warum?

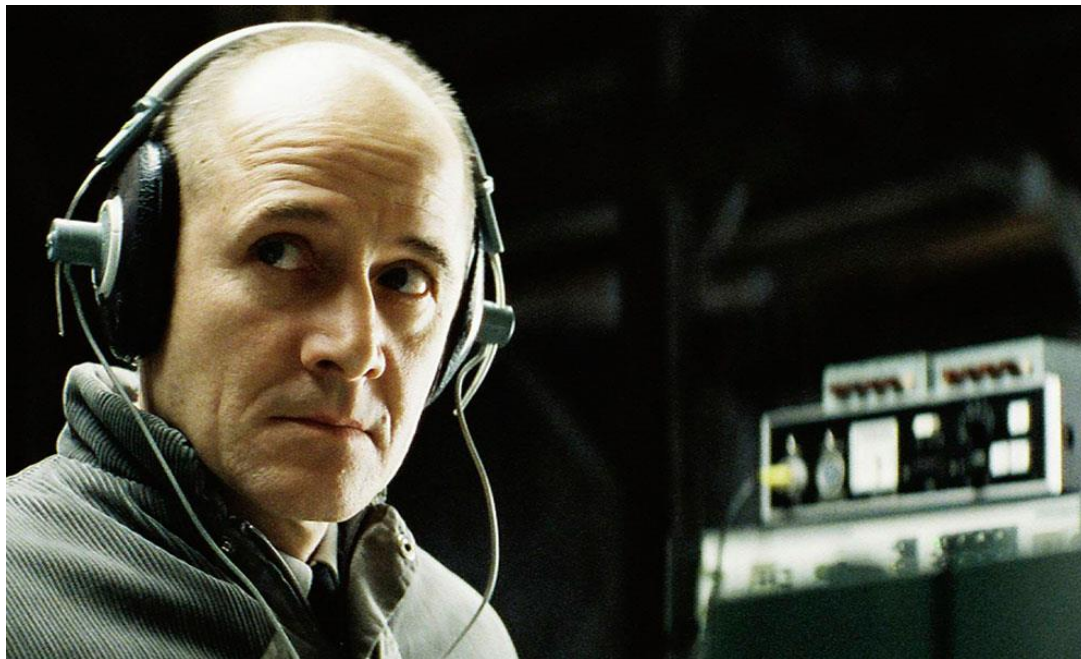


- Moral Machine vom MIT: <http://moralmachine.mit.edu/hl/de>

# Need moar Ethik?

Das Leben der Anderen

Haus des Geldes (Serie)



© ARD



© Netflix



# Need noch moar Ethik?

## Rashomon (1950)



Aus psychologischer Sicht steht die Existenz der Realität zwar nicht zur Debatte, aber ihre Widerspiegelung durch direkte und indirekte Beobachter, die sich vom Geschehen ihre eigenen gedanklichen Konstrukte bilden, werden bedeutsam.

Das Phänomen wird heute mitunter als Rashomon-Effekt bezeichnet, ist jedoch in wissenschaftlich ausgearbeiteter Form in anderen Theorien zum Beispiel als **kognitive Verzerrung** oder **selektive Wahrnehmung** bekannt. (Quelle Wikipedia)



Verantwortung!



# Entwickler

- Softwareentwicklung in KRITIS Umgebungen
- Long story short, einmal von A bis Z:
- **Secure Software Development Life Cycle (SDCL)**
  - OWASP Secure Software Development Lifecycle Project
  - Microsoft Security Development Lifecycle

# Entwickler

- Softwareentwicklung in KRITIS Umgebungen
- **Safety Integrity Level** nach IEC 61508/IEC61511
  - „Vier wohlunterschiedene Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität von Sicherheitsfunktionen, die dem E/E/PE-sicherheitsbezogenen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt.“



# Administratoren

- Administration in KRITIS Umgebungen
- Deja vu! Long story short, nochmal von A bis Z:
- Informationssicherheitsmanagementsystem (**ISMS**)
  - Angelehnt an ISO 27001, BSI Grundschutz-Kompendium
  - BSI ICS-Security-Kompendium
  - Branchenspezifischer Sicherheitsstandard (**B3S**) gemäß § 8a (2) BSIG

# Administratoren

- Administration in KRITIS Umgebungen
- B3S gemäß § 8a (2) BSIG?
  - Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt
  - 1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
  - 2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.



# Responsible Disclosure

- **Schwachstellen** sind (natürlich auch) in **KRITIS** enthalten
- Bei Fund: **Responsible Disclosure**\*
- Warum? **Versorgungsengpass oder –ausfall** möglich!
- **Halvar Flake** hat RD mal schön zusammengefasst:  
<http://addxorrol.blogspot.com/2019/08/rashomon-of-disclosure.html>

# Risiken für KRITIS





# Hackback

- Unsere **Bundesregierung** nennt es anders...
- Aktive Abwehr von Cyberangriffen oder auch **aktive Cyberabwehr**
- unter Einsatz von **digitalen Waffen**
- für den **hybrid Warfare**

# Digitale Waffen?!

- Unterschied **Security Research** und **digitale Waffen**?
  - nicht die technische Schwachstelle, sondern das Ziel!
- Forschung endet z.B. bei der Remote Code Execution (durch ausführen von calc.exe)
- Forschung biegt dann ab, Richtung Mitigation
- **D-Waffen** Entwicklung fängt dann erst richtig an...

# Gesetzgebung zu Hackback

- Alles halt nicht so einfach...
  - Völkerrecht
  - Grundrecht
  - Genfer Konventionen
- Legal... Illegal... Ikearegal...



# Hyper^^Cyber! Cyber!

- KDOCiR (Kommando Cyber- und Informationsraum)
  - Zentrum Cyber Operationen (ZCO)
    - Kernauftrag des ZCO ist das Planen, Vorbereiten und **Führen** von Cyber-Operationen (CO) zur Aufklärung und **Wirkung** (durch Cyber-Wirkketten)

Interne Verbands-  
abzeichen:



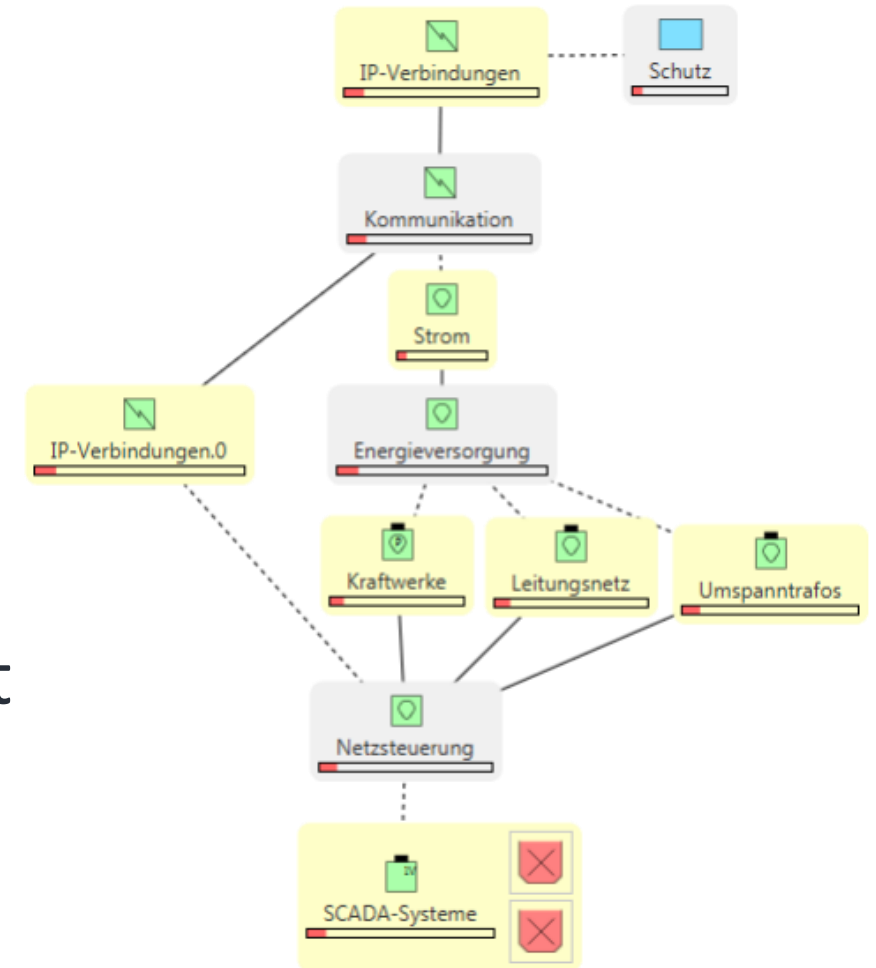
KDOCiR



ZCO

# Cyber-Wirkketten?

- **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**



# Cyber-Wirkmittel?



## Annahme



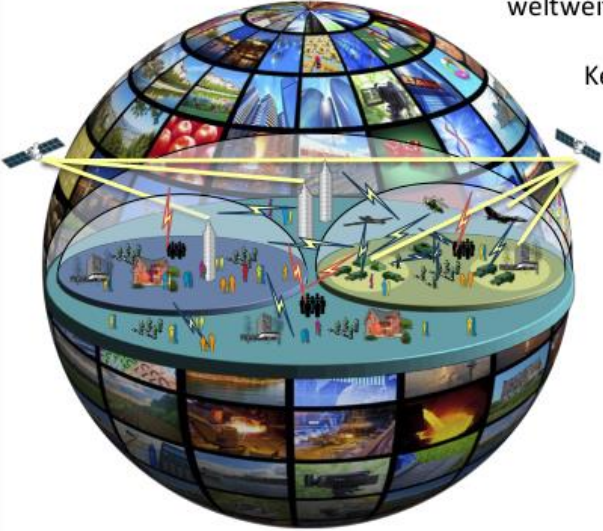


# Cyber-Wirkmittel!

KdoCIR



## Cyber-Wirkmittel



Globale Reichweite bei sofortiger Wirkung ohne Vorwarnzeit

Hohe Genauigkeit bei gleichzeitiger Bekämpfung weltweit verteilter Ziele

Kein Exponieren des Angreifers beim Einsatz der Wirkmittel

Hohe Wirkbreite ähnlich zu ABC-Wirkmitteln

Reversible Wirkung bei minimalem Kollateralschaden

Langer Vorlauf durch notwendige Eindring-/Ausbring-Phase

ähnlich einer Neutronenwaffe ohne Fall-Out

**CIR** | CYBER- UND INFORMATIONSRAUM

OFFEN

Folie 12

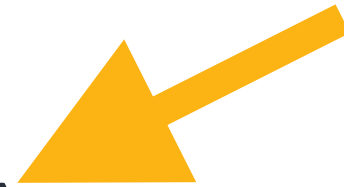
Na sag ich doch...  
das KDOCiR auch!

# Cyber-Optionen im militärischen Umfeld

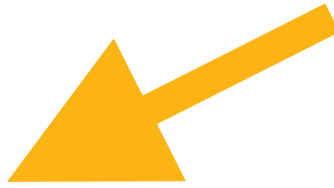
- Cyber-Optionen

- **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

Wait... wat?!?



# Charakteristik Hybrider Bedrohungen

- **Unterhalb der Schwelle eines bewaffneten Konflikts**
  - **Verschleierung** der Urheberschaft zur Vermeidung der Attribution
  - Konzertierte **Desinformationspolitik**
  - **Destabilisierung** einer Gesellschaft von innen
- Öhm?!?
- 



# Hybrid Warfare und Hackback

- Gelebt wird eine **wissenschaftsfeindliche Sicherheitspolitik** (wie bei der Klimapolitik)
- Resultat: Mehr Security?
- Nope -> mehr Cyber**UN**sicherheit

# Ach komm... wissenschaftsfeindliche Sicherheitspolitik?

## *Geheimes Bundestagsgutachten attackiert Hackback-Pläne der Bundesregierung*

- Der **Wissenschaftliche Dienst** sagt „Die Bundesregierung arbeitet an offensiven Kapazitäten und Hackbacks, doch das ist **ineffektiv** und **gefährlich**.“
- Entwickelt hat es Dr. John Zimmermann **Oberstleutnant** der Bundeswehr
- Steht seit **über 30 Jahren** im Dienst der Bundeswehr
- Es wurden **wesentliche Teile** der Forderungen der **AG KRITIS** bestätigt



Das **Gutachten** wurde auf **netzpolitik.org** veröffentlicht.

18 Seiten harter Tobak!

**NETZPOLITIK** ● **ORG**

Quelle: <https://netzpolitik.org/2019/geheimes-bundestagsgutachten-attackiert-hackback-plaene-der-bundesregierung/#spendenleiste>

# Physische Auswirkungen auf KRITIS?

## 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**



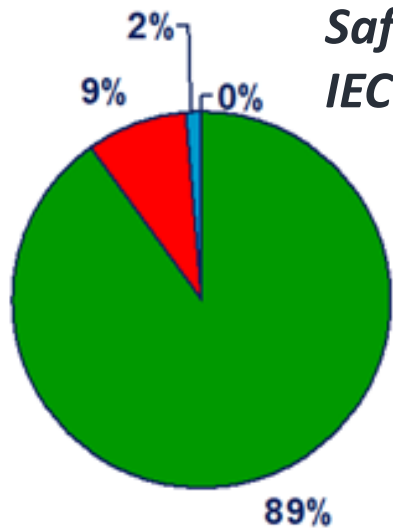


# Aurora Generator Test am INL

## Official Use Only

Contains information which may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number (s) 2 . Approval by the Department of Energy prior to public release is required.

Reviewed by: Thomas Harper 03/5/07



**Safety Integrity Level  
IEC 61508/IEC61511**

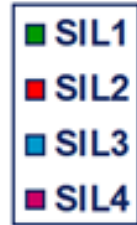


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.



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

## Attacken auf das Ukrainische Stromnetz

- Auswirkungen: ca. 250.000 betroffene Personen in Kiew und dem Umfeld

## Angriff auf Saudi Arabisches Kraftwerk

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

Und nun?





A close-up photograph of a person's hand holding a small, round, silver compass. The hand is positioned palm-up, with the thumb and index finger supporting the compass. The compass face is black with white markings for degrees and cardinal directions (N, NE, E, SE, S, SW, W, NW). The needle is white with a red tip. The background is dark and out of focus.

Unabhängigkeit des BSI vom BMI

Strikt defensive Cybersicherheitsstrategie

Ächtung von ABCD-Waffen (inkl. Digitalen Waffen)

Evaluierung der vorhandenen Gesetze und Maßnahmen

Bevölkerungsschutz durch Behebung von Schwachstellen durch Hersteller



# Defensive Cybersicherheitsstrategie

- Bei KRITIS eingesetzte Software grundsätzlich als Open Source oder Quellcode in treuhänderischer Verwaltung
- Bildungspolitik: Sichere(!) Quellcode-Entwicklung ausbilden
- Keine Bereitstellung von Budgets für staatliche Akteure, um 0days zu kaufen oder zu entwickeln
- Verpflichtung für staatliche Akteure, ihnen bekannt gewordene Schwachstellen über ein unabhängiges BSI an den Hersteller zu melden

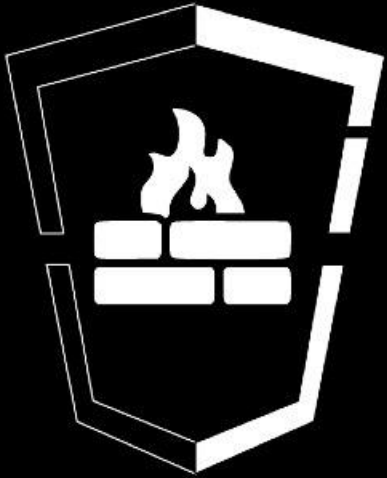
# Unabhängigkeit des BSI

Evaluierung möglicher Optionen:  
(fachliche Unabhängigkeit, starke Unabhängigkeit,  
andere Abhängigkeit, Digitalministerium, ...)

Vielversprechende Option: § 1 BSIG Änderung zur  
Grundlage technisch-wissenschaftlicher Erkenntnisse  
*„Das BSI führt seine Aufgaben auf der Grundlage  
wissenschaftlich-technischer Erkenntnisse nach den  
Anforderungen der jeweils fachlich zuständigen Ministerien  
durch.“*



# What's Next?



# DefensiveCon

**v02: 07-08 February 2020 / c-base Berlin**



 @HonkHase

HonkHase@kritis.info

www.blablasecurity.de

ag.kritis.info



Stickaz!

