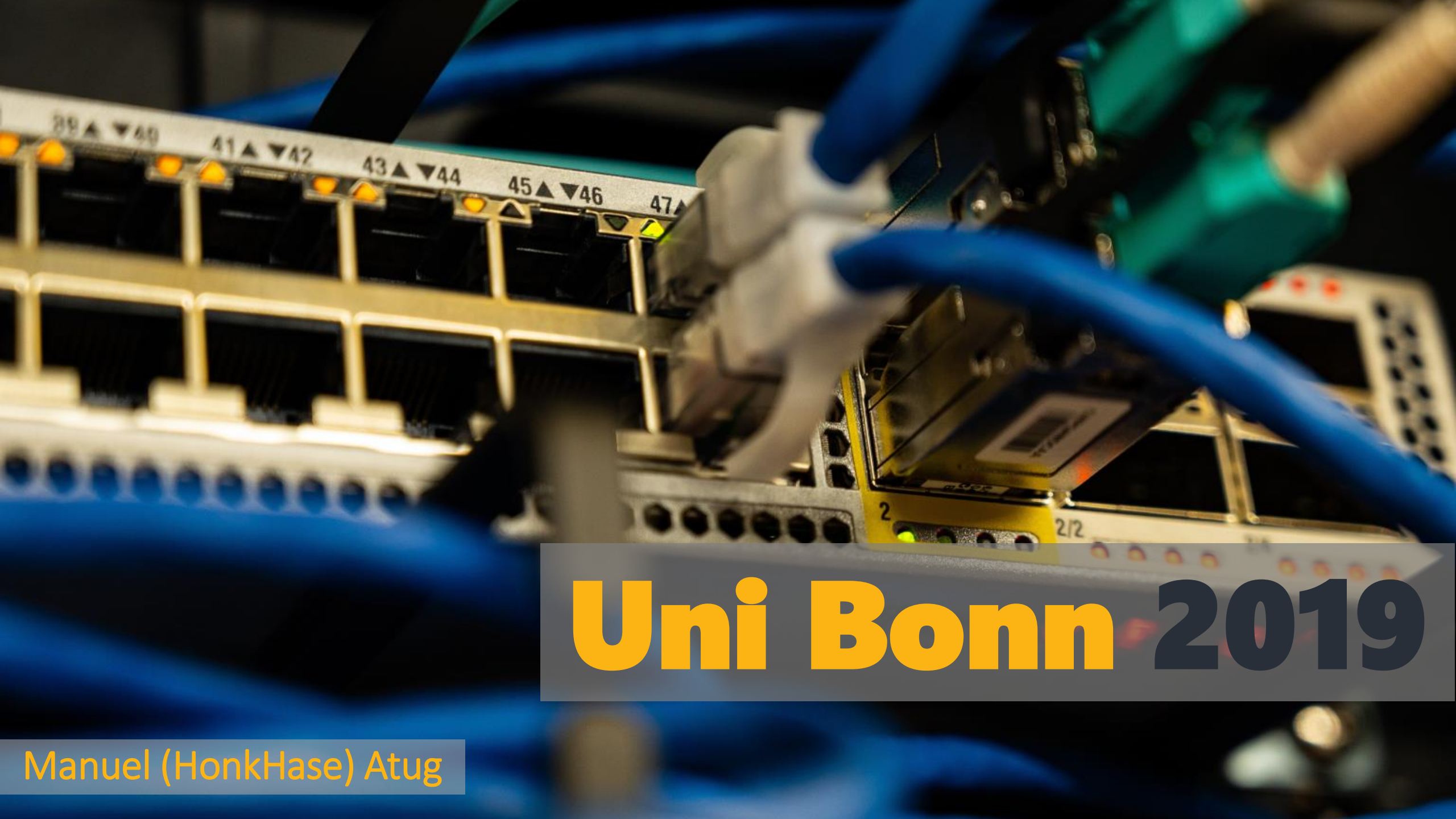


Uni Bonn 2019

Manuel (HonkHase) Atug

Responsible Disclosure und Hackback aka Ethik Rekalibrieren

Manuel (HonkHase) Atug

Manuel (HonkHase) Atug

Ich habe #KRITIS im Endstadium

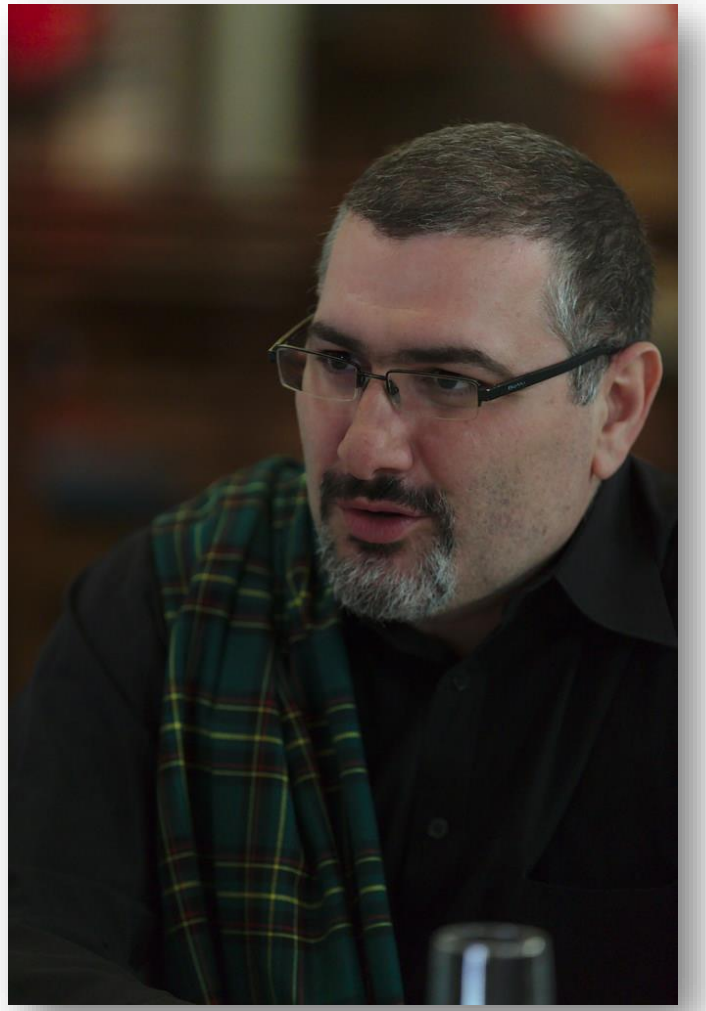
Senior Manager bei der HiSolutions AG

- 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., FIfF 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

AG KRITIS



Was ist Ethik (vs. Moral)?

Begriffsbestimmung

Moral

- Gesamtheit von ethisch-sittlichen Normen, Grundsätzen, Werten, die das zwischen-menschliche 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?

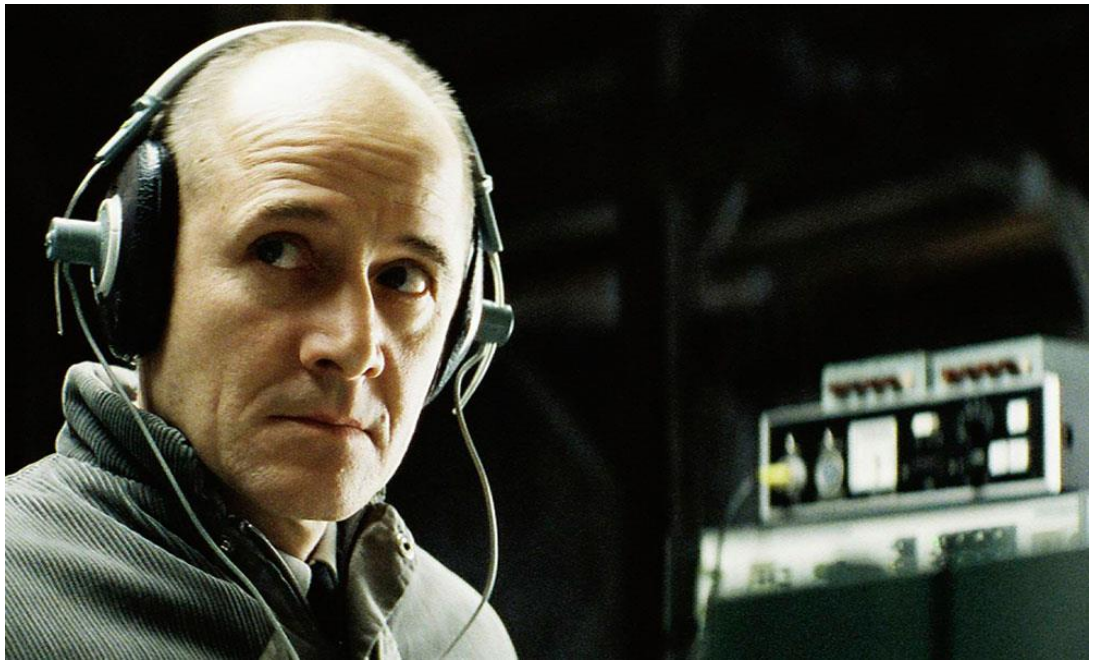
- Moral Machine vom MIT: http://moralmachine.mit.edu/hl/de

Offensive vs Defensive

- **Offensive** Security vs. **Defensive** Security
- For the win! Bei **Capture the Flag** (CTF) ist **Offensive** erforderlich. Oder nicht?
- Damals beim ersten CTF auf dem **CCC Congress**…

Need moar Ethik?

Das Leben der Anderen



© ARD

Haus des Geldes (Serie)

© 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)

Responsible Disclosure

Responsible Disclosure vs Full Disclosure

Responsible Disclosure

- Betroffener Hersteller wird informiert
- Hersteller bekommt Zeit für die Behebung
- Erst danach wird veröffentlicht

Full Disclosure

- Zeitgleich Veröffentlichung bzw. Offenlegung

Responsible Disclosure

- **Schwachstellen** sind in allen Systemen enthalten
- Gefunden! **Responsible Disclosure**, klarer Fall!
- Warum? **Versorgungsengpass oder –ausfall** möglich!
- Wie? Via Hersteller oder CERT, klar!

Responsible Disclosure

- Oder doch nicht?
  „die Bösen™“ nutzen dann offene Schwachstellen!

- Well… irgendwie also schon melden, aber wie?

- Schöne Zusammenfassung der Problematiken von **Halvar Flake** http://addxorrol.blogspot.com/2019/08/rashomon-of-disclosure.html

Responsible Disclosure

- Alternativen anyone?
- I can haz Phun for Profit -> 0day selling / trading… die bessere Option?

Preisliste für 0days

Capabilities	Apple iOS
Component	Any default component
First stage	Remote Code Execution
Second stage	Privilege Escalation
Interaction	**No user interaction**
Persistency	✔
Payout	**Up to 4.0M USD**

Second stage	Sandbox Escape and Privilege Escalation	Privilege Escalation	Privilege Escalation	Privilege Escalation
Interaction	Browse a web page	**No user interaction**	Run exploit in VM	Run exploit in VM
Payout	**Up to 1.5M USD**	**Up to 1.0M USD**	**Up to 500K USD**	**Up to 250K USD**

Bugfense Zero-Day Hitlist http://bugfense.io/index.html

Hackback

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

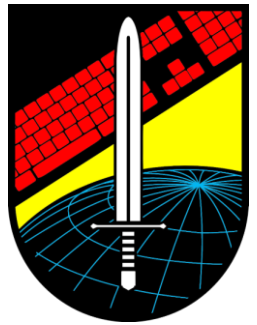
- Legal… Illegal… Ikearegal…

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:

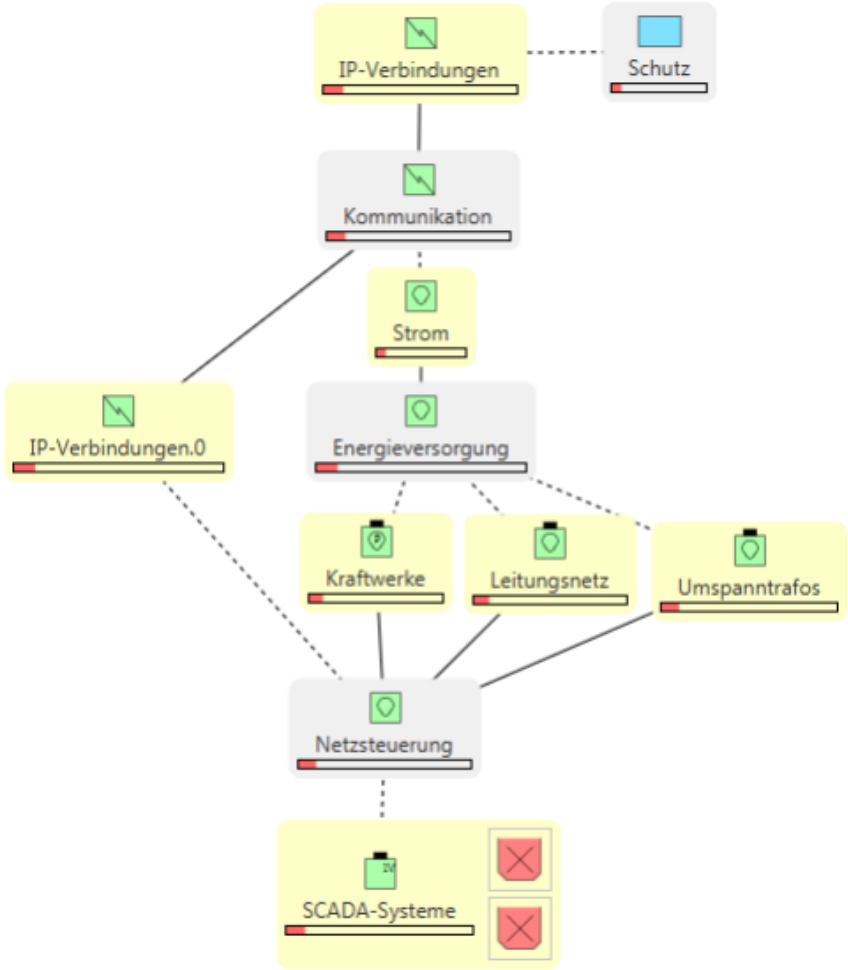
KDOCiR



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!

KdoCIR

Cyber-Wirkmittel

Globale Reichweite bei sofortiger Wirkung ohne Vorwarnzeit

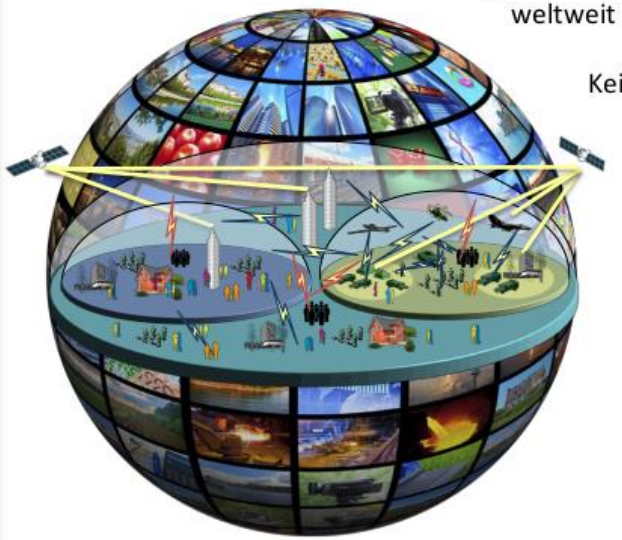
Hohe Wirkbreite ähnlich zu ABC-Wirkmitteln

Hohe Genauigkeit bei gleichzeitiger Bekämpfung weltweit verteilter Ziele

Reversible Wirkung bei minimalem Kollateralschaden

Kein Exponieren des Angreifers beim Einsatz der Wirkmittel

Langer Vorlauf durch notwendige Eindring-/ Ausbring-Phase



ähnlich einer Neutronenwaffe ohne Fall-Out

CIR CYBER- UND INFORMATIONSRAUM OFFEN Folie 12

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

Charakteristik Hybrider Bedrohungen

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

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

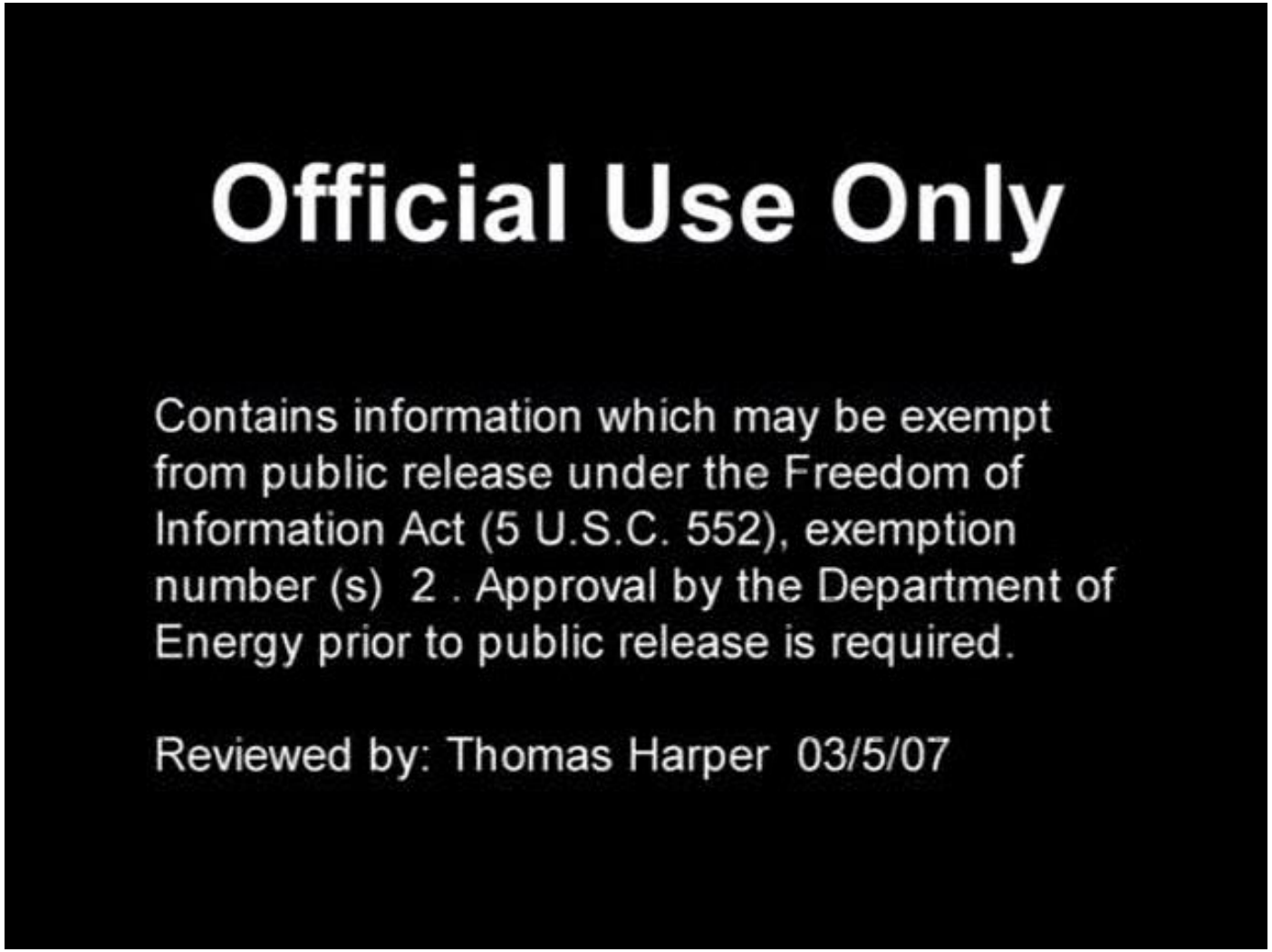
Physische Auswirkungen auf KRITIS?

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



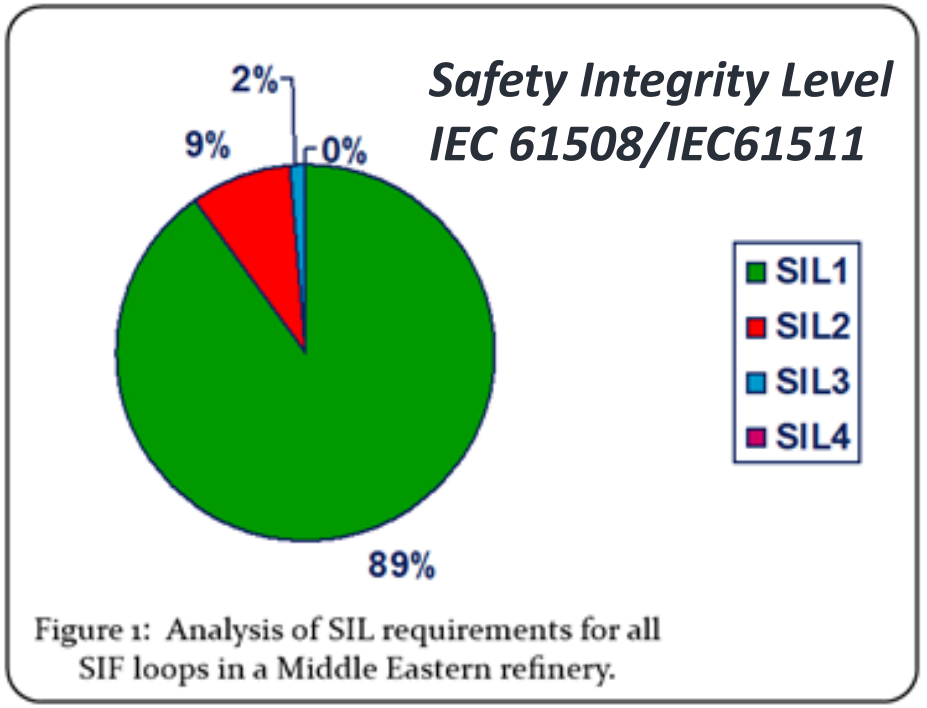


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.

Triconex Tricon

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

Attacke auf Saudi Arabisches Kraftwerk

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

Und nun?

Für einen persönlich: Überlegt vorher & regelmäßig immer wieder, wie Ihr damit umgehen wollt!

Ächtung von ABCD-Waffen (inkl. Digitalen Waffen)

Was geben vorhandene Gesetze und Maßnahmen her?

Ausrichtung an einer strikt defensiven Cybersicherheitsstrategie

Bevölkerungsschutz durch Behebung von Schwachstellen (durch Hersteller)

What‘s Next?

@HonkHase

HonkHase@kritis.info

www.blablasecurity.de

ag.kritis.info

Stickaz!

AG KRITIS