11.07.2018, CODE Jahrestagung – Workshop „Recht & Regulierung im Cyber- und Informationsraum“

„Digitaler Gegenangriff“
Politischer Diskurs in Deutschland und den USA

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Hackback

Aktive Cyber-Abwehr

Zurückcybern

Eine aktive Gegenmaßnahme, die dazu ausgelegt ist einen Cyber-Angriff abzuwehren und/ oder aufzuklären.

**Eigene Definition*

Digitaler Gegenangriff

Finaler Digitaler Rettungsschuss

Passive Verteidigung

Prävention (z. B. Firewalls, Antivirus)

Informationen sammeln - passiv (z. B. Honeypots)

Aktive Verteidigung

Datenfallen – nicht-invasiv (z. B. Canary Tokens oder Non-Invasive Beacons)

ISP Unterstützung (Blocken, Rerouten, Umlenken z. B. von DDoS-Angriffen)

Informationen sammeln – aktiv (z. B. durch nachrichtendienstliche Aktivitäten gegen IXP)

Übernahme der externen Infrastruktur

Hosting und ISP Unterstützung bei einem (international) koordinierten Botnet-Takedown (z. B. durch Sink Holing, forensischer Analyse oder Data Recovery)

ISP Unterstützung um Kommunikation mit Bots zu unterbinden (z. B. Walled Garden)

Übernahme von Systemen (z. B. Command-und-Control um Bot-Rechner zu desinfizieren)

Infiltration interner Infrastruktur

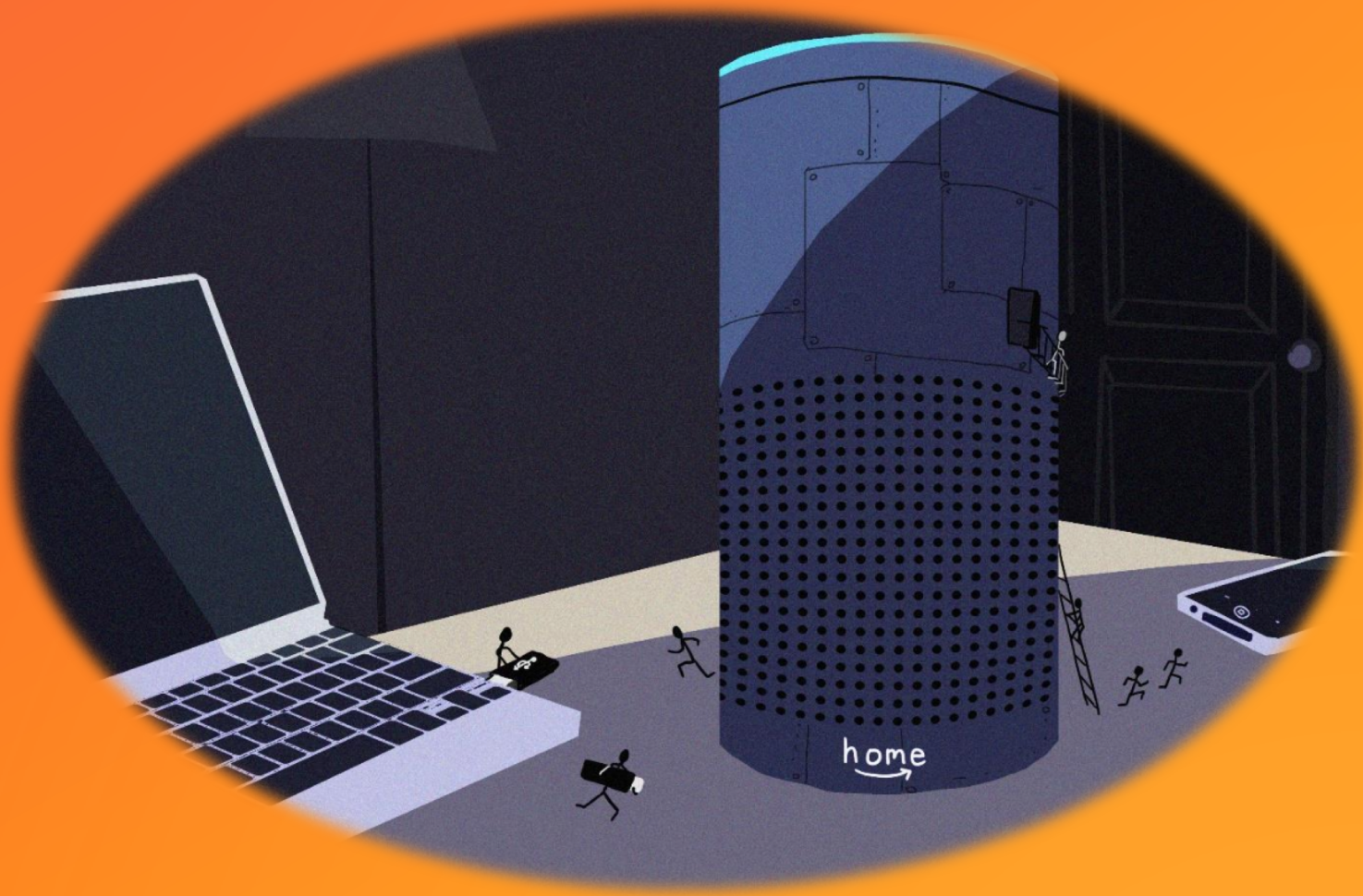
Datenfallen – invasiv (z. B. Verschlüsselung oder Löschung von Zielsystemen)

Aufklärung in Systemen (z. B. Werkzeuge, aber auch Kameras und weitere Sensoren)

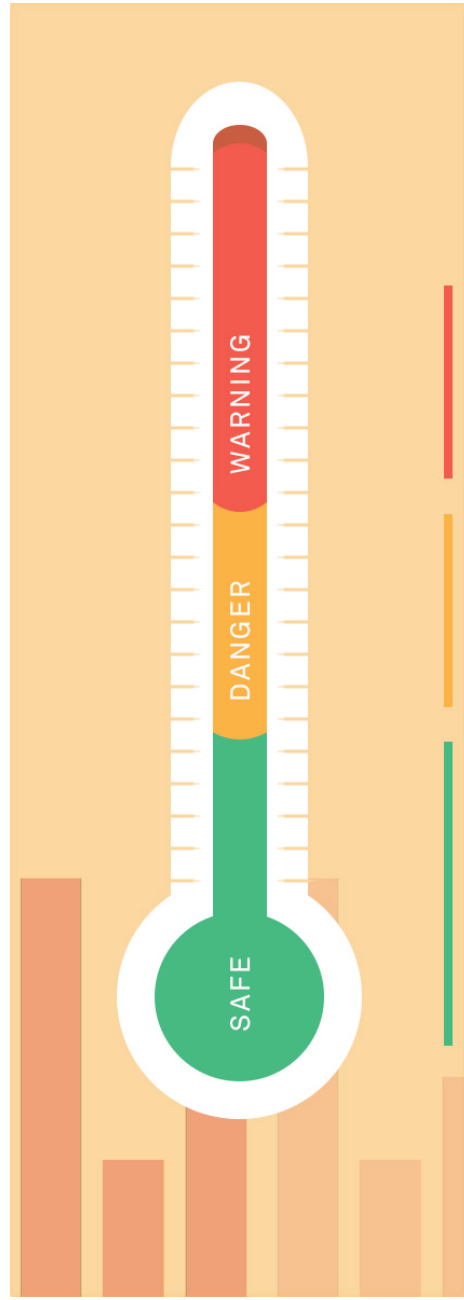
Löschung gestohlener Daten in Systemen

Temporäre Disruption von Systemen

Langfristige Disruption von Sytemen (z. B. Bricking)




E PLURIBUS UNUM



Invasiveness of Hackback-Activities

(NOMENCLATURE)

"Destruction" of Systems
Disruption of Systems
Data Deletion in Systems
Reconnaissance in Systems

Bot Vaccinations
Invasive Beacons
Active Intelligence
Pro-Active ISP Assistance

ISP and Host Assistance for Takedowns
Reactive ISP Assistance
Non-Invasive Beacons
Passive Intelligence
Prevention Mechanisms

Stiftung Neue Verantwortung

Dr. Sven Herpig
Leiter “Internationale Cyber-Sicherheitspolitik”
Projektleiter “Transatlantic Cyber Forum” (TCF)

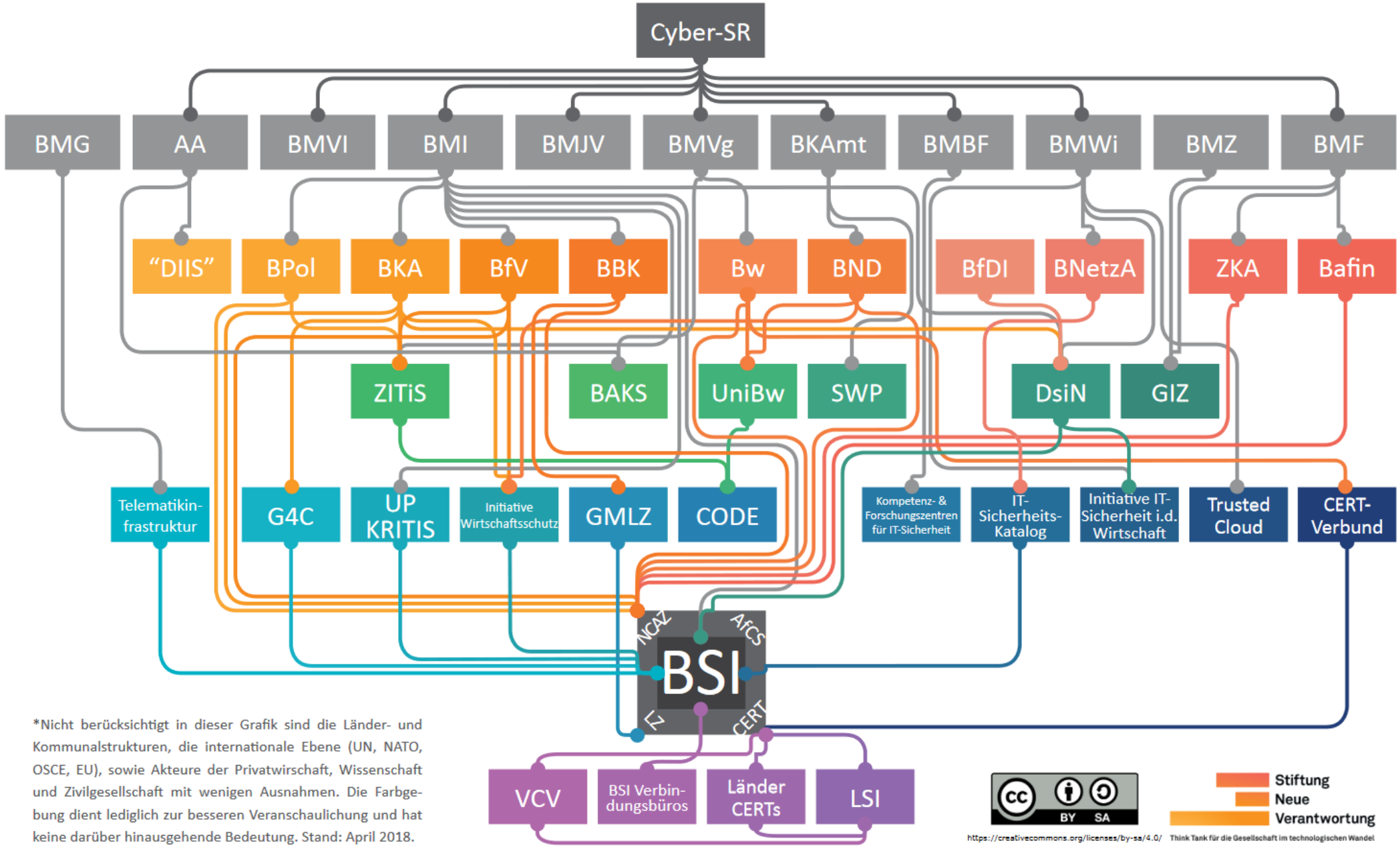
sherpig@stiftung-nv.de
@z_edian (Twitter)

Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

Think Tank für die Gesellschaft im technologischen Wandel

Stiftung
Neue
Verantwortung

Staatliche Cyber-Sicherheitsarchitektur*



*Nicht berücksichtigt in dieser Grafik sind die Länder- und Kommunalstrukturen, die internationale Ebene (UN, NATO, OSCE, EU), sowie Akteure der Privatwirschaft, Wissenschaft und Zivilgesellschaft mit wenigen Ausnahmen. Die Farbgebung dient lediglich zur besseren Veranschaulichung und hat keine darüber hinausgehende Bedeutung. Stand: April 2018.

Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel