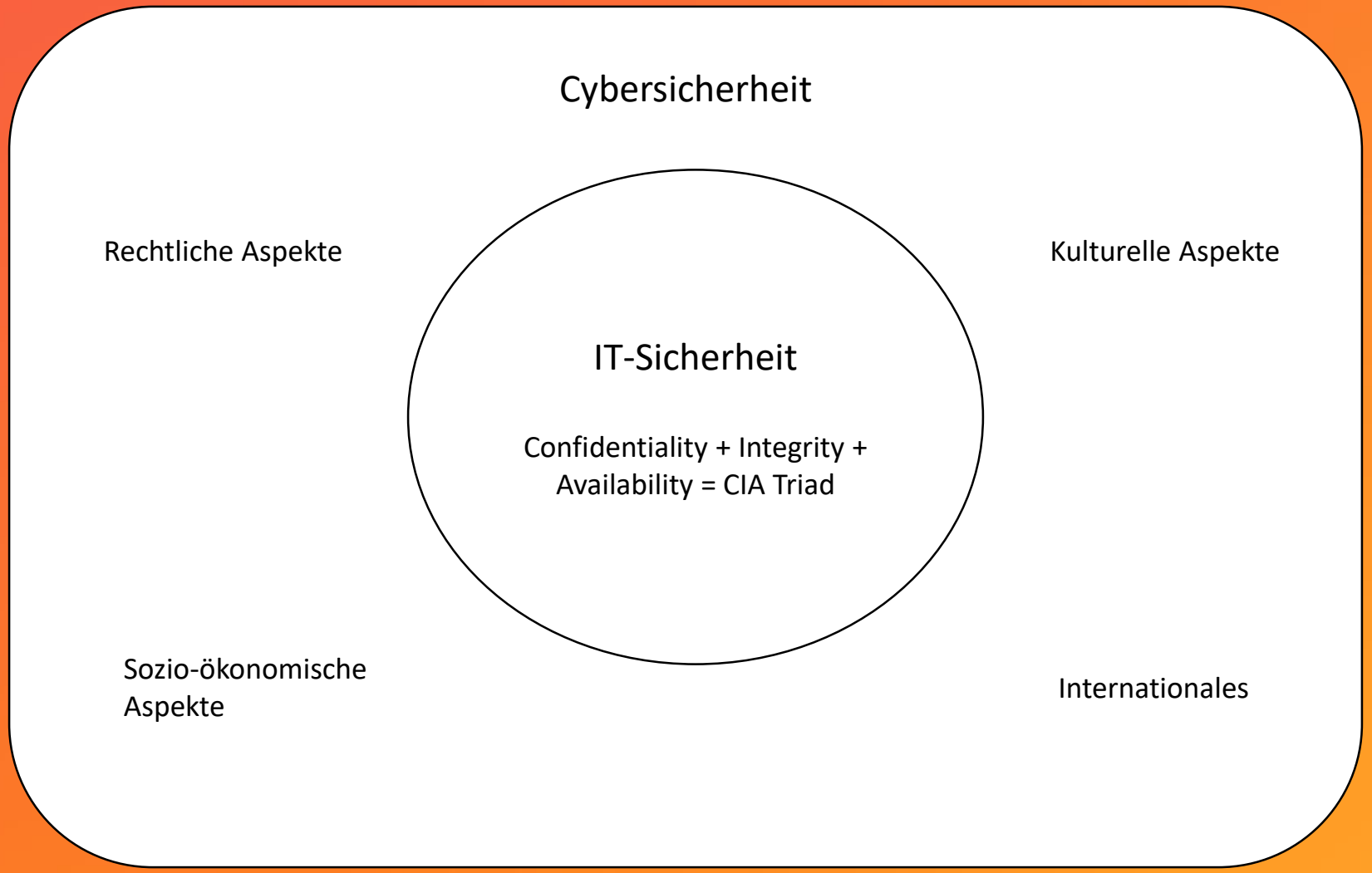
08.02.2020: DefensiveCon, c-base

Cybersicherheitsstrategie 2021: Resilienz statt Cyberstrategieunfähigkeit

Stiftung Neue Verantwortung

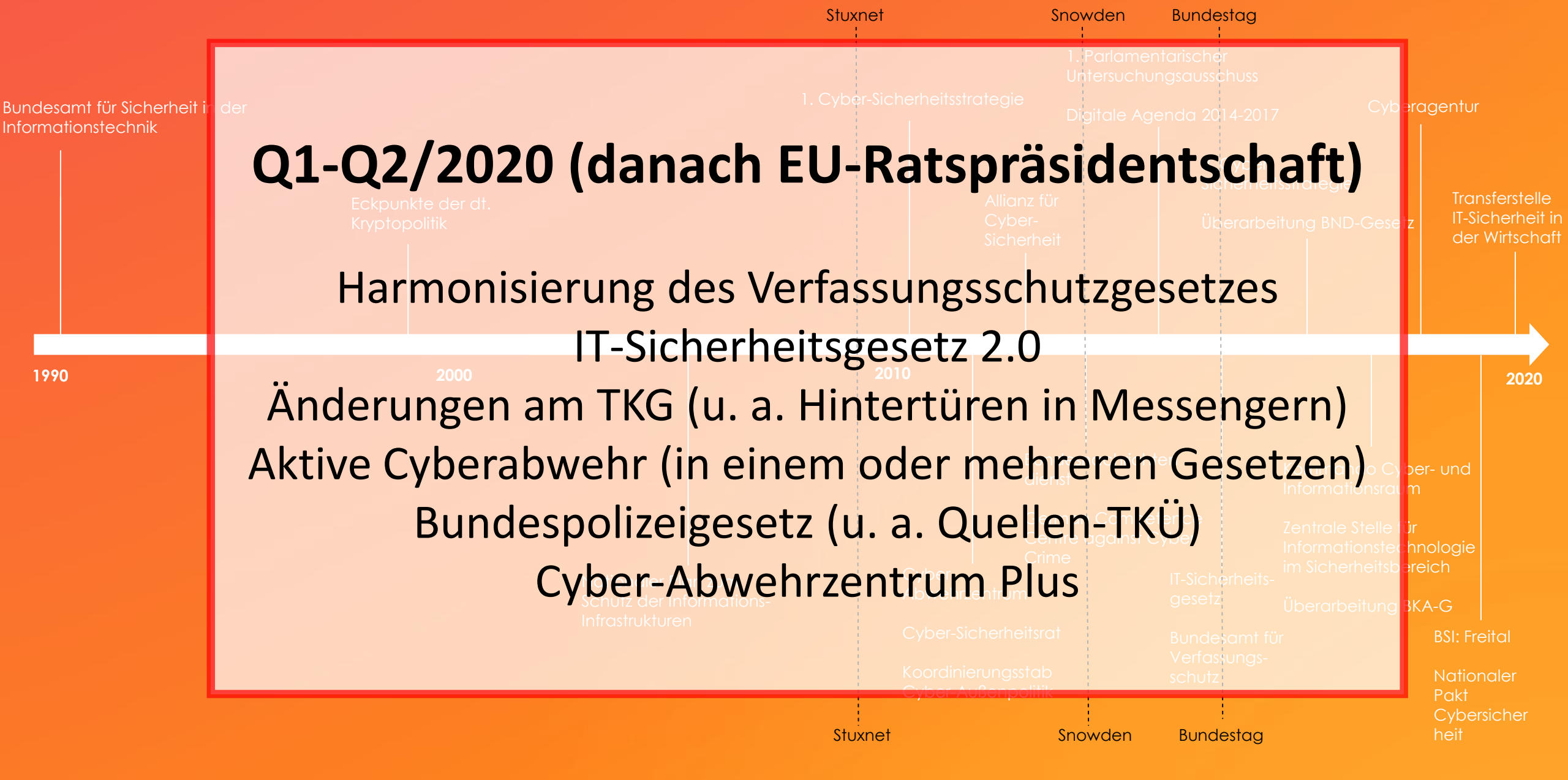
Think Tank für die Gesellschaft im technologischen Wandel

Cybering all Cybers

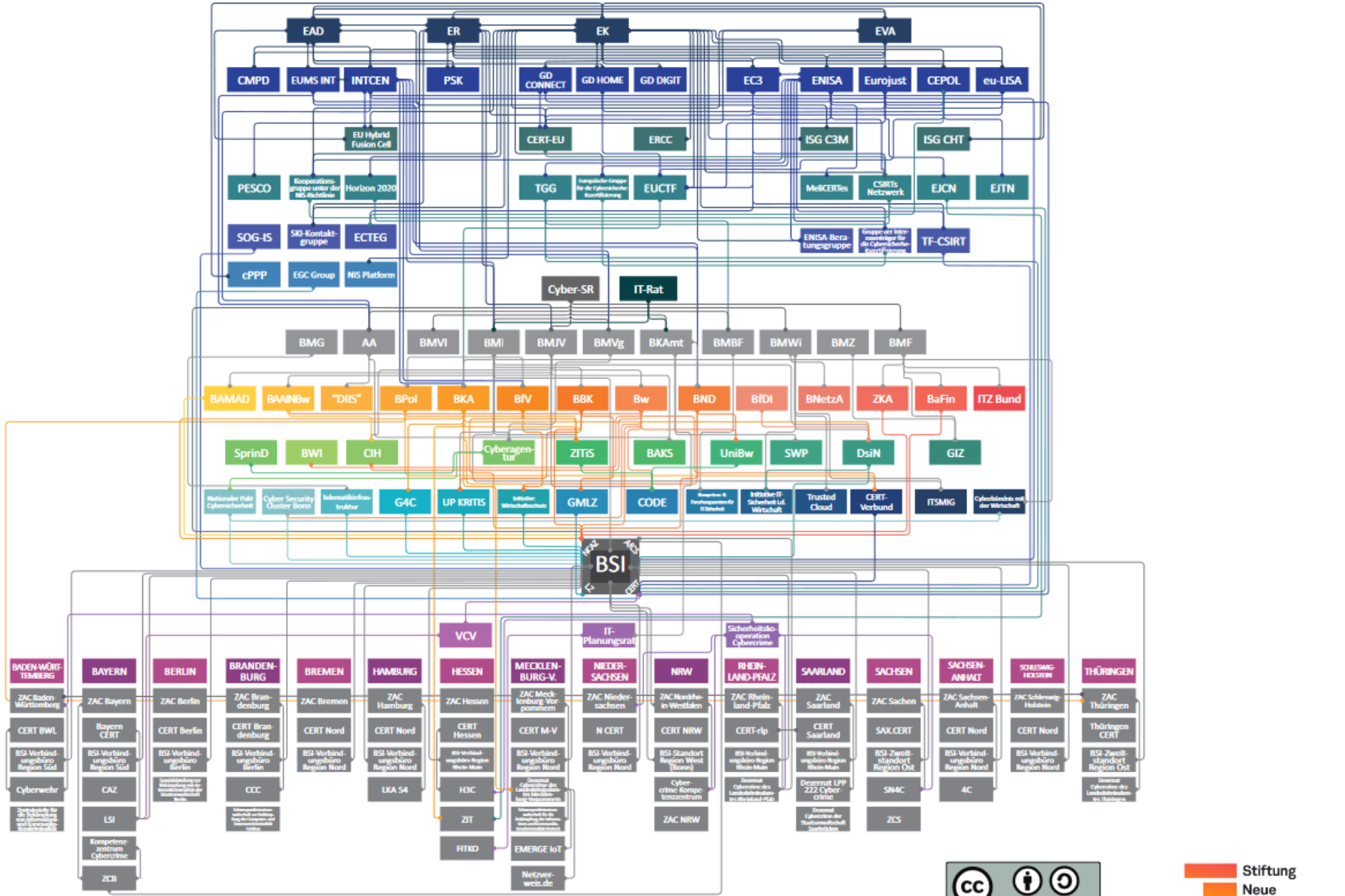


Cybersicherheitspolitik in Deutschland 1991-2020

Entwicklung der Cybersicherheitspolitik



Staatliche Cybersicherheitsarchitektur



Cybersicherheitsstrategien 2011 & 2016

Cyber-Sicherheitsstrategie für Deutschland 2011

Vorgehen:	Ein Ressort (BMI)
Veröffentlichung:	2011
Maßnahmen:	10
Besonderheiten:	- Strategische Leitlinien (u. a. Primat des Zivilen, Umfassender Ansatz, Nationale/International) - Nachhaltigkeit (Cyber-SR) - Mini-Glossar - Wurde durch CSS2016 außer Kraft gesetzt
Budget:	0 Euro
Bewertung:	- “Minimum Viable Product” als Maßnahmenpaket mit guten Ansätzen, z. B. Personalentwicklung und Schaffung zentraler Institutionen (Cyber-SR/-AZ) - Keine Evaluation - Keine wirkliche Strategie

Cyber-Sicherheitsstrategie für Deutschland 2016

Vorgehen:	“Whole-of-Government” unter BMI-Federführung
Veröffentlichung:	2016
Maßnahmen:	29 in 4 Bereichen (Verbraucher und Souveränität, Staat, Wirtschaft, Internationales)
Besonderheiten:	- Strategische Leitlinien (u. a. Risikoangemessenheit, Gemeinsame Verantwortung, National/International) - Nachhaltigkeit durch Cyber-SR Umbau - Mini-Glossar
Budget:	0 Euro
Bewertung:	- Adressiert aktuelle Herausforderungen - Primat des Zivilen fehlt - Vermischung von öffentlicher Sicherheit und IT-Sicherheit - Offensive Maßnahmen für IT-Sicherheit (u. a. SIGINT Support to Cyber Defense) - “Giftschrank”-Maßnahmenpaket - Keine Evaluation vorgesehen - Keine wirkliche Strategie

tl;dr: Wir brauchen eine (neue) Strategie

1. Strategieunfähig (Architektur, Beantwortung, Vision)
2. “Wissenschaftsfeindliche” Gesetzgebungsvorhaben (u.a. aktive Cyberabwehr, Hintertüren)
3. Ressortstreitigkeiten (u.a. Cyberfähigkeitsaufbau im Ausland)
4. Evaluationsunwilligkeit der Exekutivbehörden
5. Fachkräftemangel und -verschwendung (u.a. "Hackbacks“, Mobile “Cyberteams”)
6. Vermengung von öffentlicher Sicherheit und IT-Sicherheit als "Cybersicherheit"
7. Zentrale Akteure der deutschen Cybersicherheitsarchitektur weisen Schwächen auf:
   I. Aufgabe, Arbeitsweise und Einbindung in den zentralen strategischen Akteur (Cyber-SR) sind schwer nachzuvollziehen (u.a. Gesellschaft fehlt)
   II. Der zentrale koordinierende Akteur (Cyber-AZ) ist offenbar reformunfähig und hat [illegible]
   III. Einer der zentralen operativen Akteure (BSI) wird aus politischem Kalkül bei seiner eigentlichen Arbeit beeinträchtigt (u.a. fragwürdige 2. und 3. Standorte)
   IV. Der zentrale Dienstleister für offensive und forensische Cyberfähigkeiten (ZITiS) hat eine normativ nicht ausreichende Rechtsgrundlage
   V. Neue Akteure wie der Nationale Pakt für Cyber-Sicherheit sind reines Opium für’s Volk

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Ausschussdrucksache
19(4)255 A

Stiftung
Neue
Verantwortung

Sachverständigenstellungnahme von Dr. Sven Herpig[1], Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, für die Sitzung des Bundestagsausschusses für Inneres und Heimat am 08.04.2019 zum Thema "IT-Sicherheit"

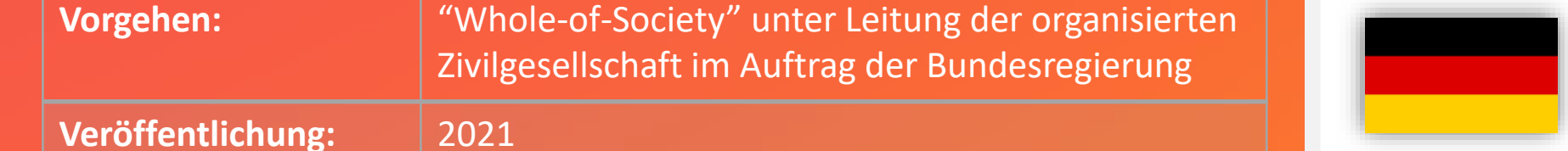
https://docs.zoho.com/file/io2apaa63245e53284d3e92c6defda8117053

Cyberresilienzstrategie 2021?

Warum „Resilienz“?

1. Gerade bei Kritischen Infrastrukturen reicht Sicherheit allein (nicht) mehr aus und muss über den digitalen Tellerrand hinaus gedacht werden.
2. Resilienz begegnet einem breiten Spektrum an Angriffsmotivationen (Sabotage, Kriminalität..)
3. Ein defensiver Ansatz der auf Resilienz fokussiert wäre ein Gegenentwurf zu den aktuell vorherrschenden Entwürfen, könnte für viele Staaten ein “Dritter Weg” sein und dadurch das Internet als Ganzes sicherer machen. Mit der deutschen Ratspräsidenschaft ab Q3/2020 könnte man ein solches Vorhaben europaweit vorantreiben.
4. Aktuelle Ansätze:
    - Defensive und offensive Maßnahmen (u. a. USA und Israel)
    - Offensive Maßnahmen, Überwachung und Abkopplung (u. a. China und Russland)
5. Aufgrund (finanzieller und personeller) Ressourcen sowie begrenztem politischem Kapital ist eine Fokussierung zielführend

Vorgehen:	“Whole-of-Society” unter Leitung der organisierten Zivilgesellschaft im Auftrag der Bundesregierung
Veröffentlichung:	2021
Maßnahmen (u.a.):	1. Konsolidierung der Cybersicherheitsarchitektur, u. a. Umbau Cyber-SR als WoS ink. Externer Expert:innen 2. Reform des Tarifrechts 3. Einbindung von deutschen (und europäischen) Expert:innen in strategische & operative Vorhaben 4. Fokus auf Stärkung der Resilienz kritischer Infrastrukturen 5. Skalierende PPP-Dienstleistungen für SMEs
Besonderheiten:	- Intersektoraler Bottom-Up Prozess - Ausführliche Strategie (Wiedereinführung des Primat des Zivilen, Resilienz-Fokus, Dritter-Weg..) - Ausführlicher Glossar (u. a. zur Unterscheidung von Öffentlicher und IT-Sicherheit - Konkrete Evaluationskriterien und Zeitrahmen - Offensive Maßnahmen lediglich für IT-Sicherheit (Pentest, Redteam …) und Non-Remote Forensik.
Budget:	Umschichtung von Personalstellen vorsehen



Cyberresilienzstrategie für Deutschland 2021

Stiftung
Neue
Verantwortung

Dr. Sven Herpig
Leiter “Internationale Cybersicherheitspolitik”
sherpig@stiftung-nv.de
@z_edian (Twitter)

Think Tank für die Gesellschaft im technologischen Wandel