TECHNISCHE UNIVERSITÄT
CHEMNITZ

Referat in Grundlagen der Internationalen Politik
von Lucas Hums und Hubertus Leo Weigel

Globales Internet, Netzpolitik, Cybersicherheit

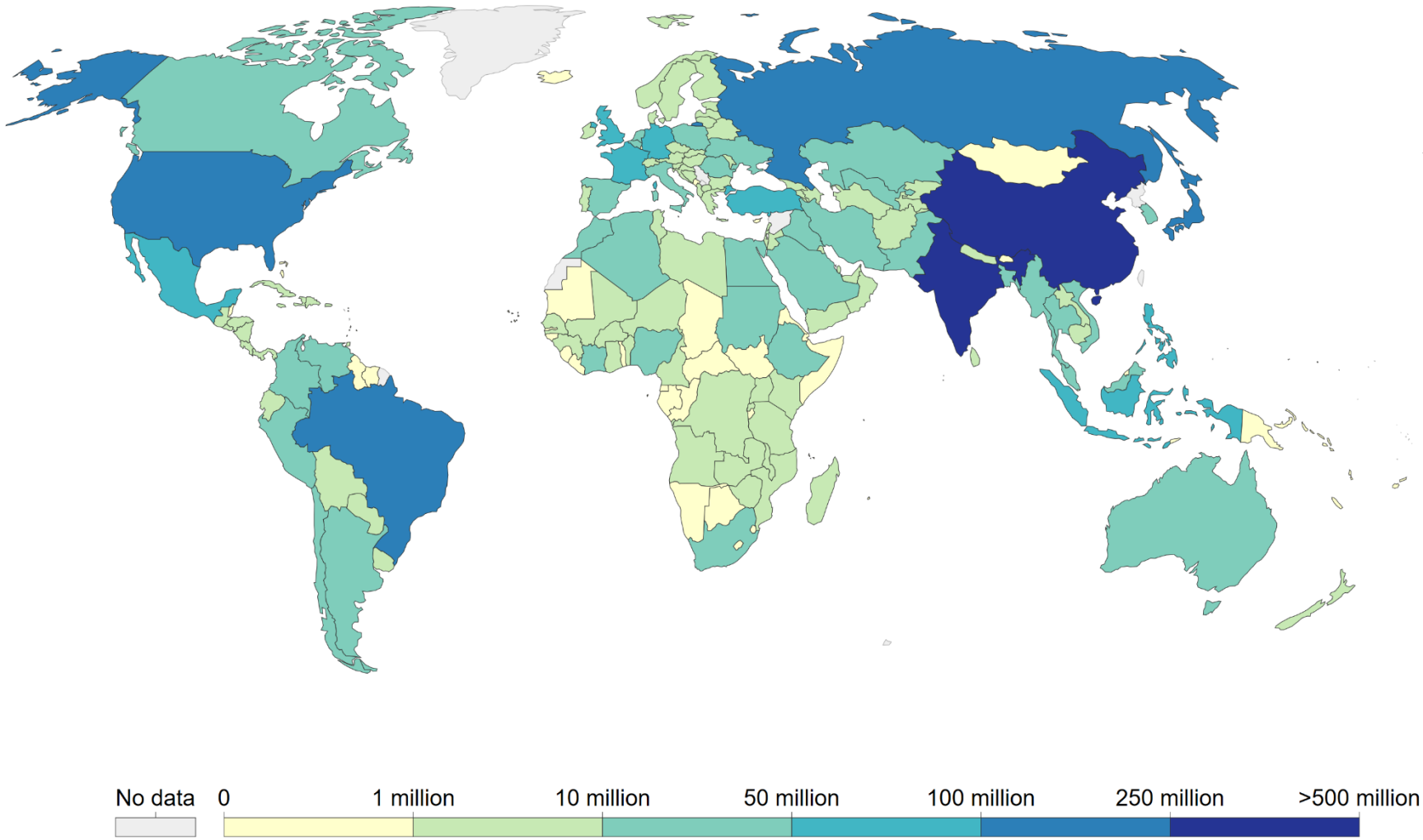
Gliederung

1 Globales Internet

[b: 1]

Globales Internet, Netzpolitik, Cybersicherheit

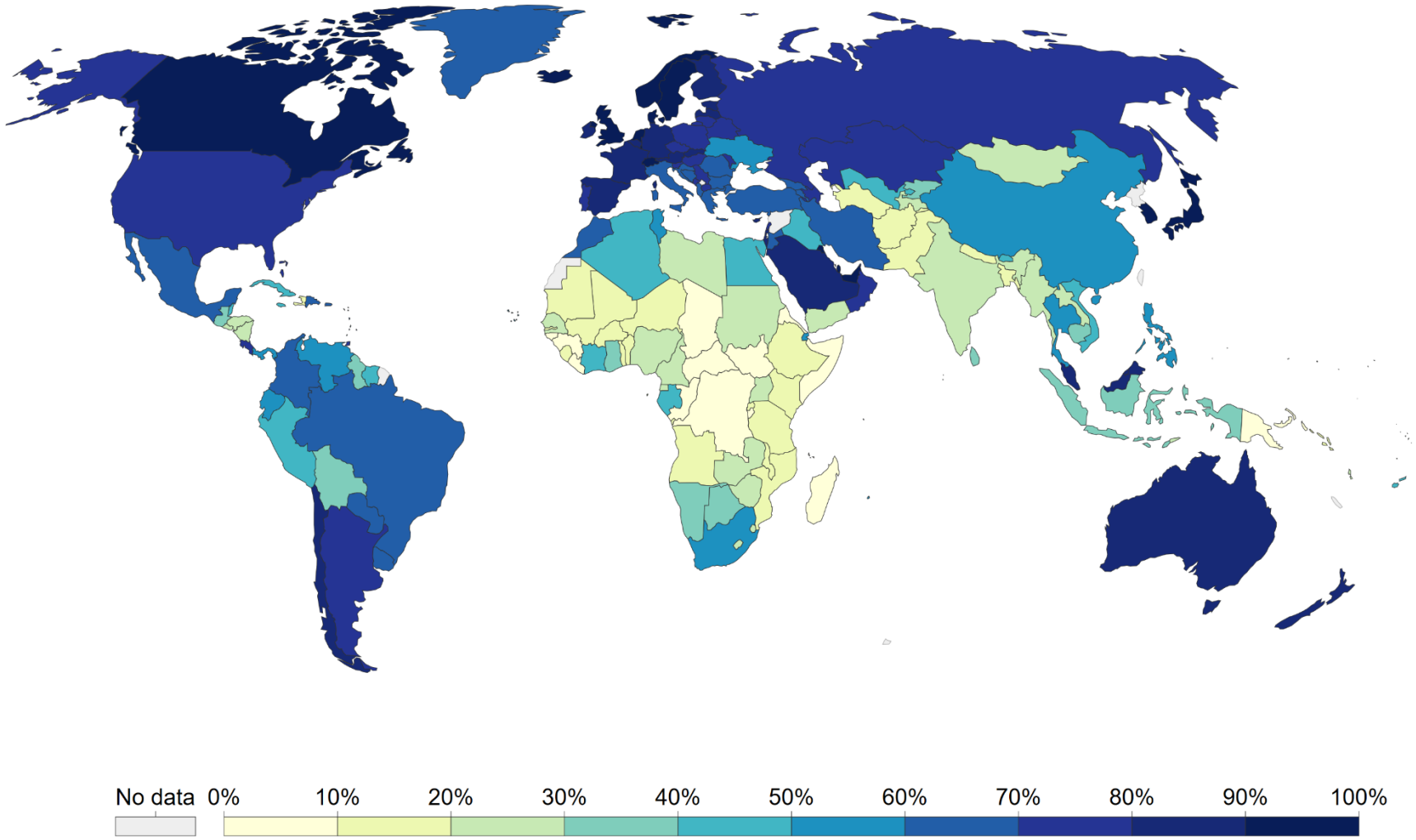
Number of internet users by country, 2017



Source: OWID based on World Bank & UN World Population Prospects (2017)

Die Anzahl der Weltweiten Internetnutzer:innen nach Land

„Internetnutzer sind Personen, die das Internet (von jedem Ort aus) in den letzten 3 Monaten genutzt haben.“

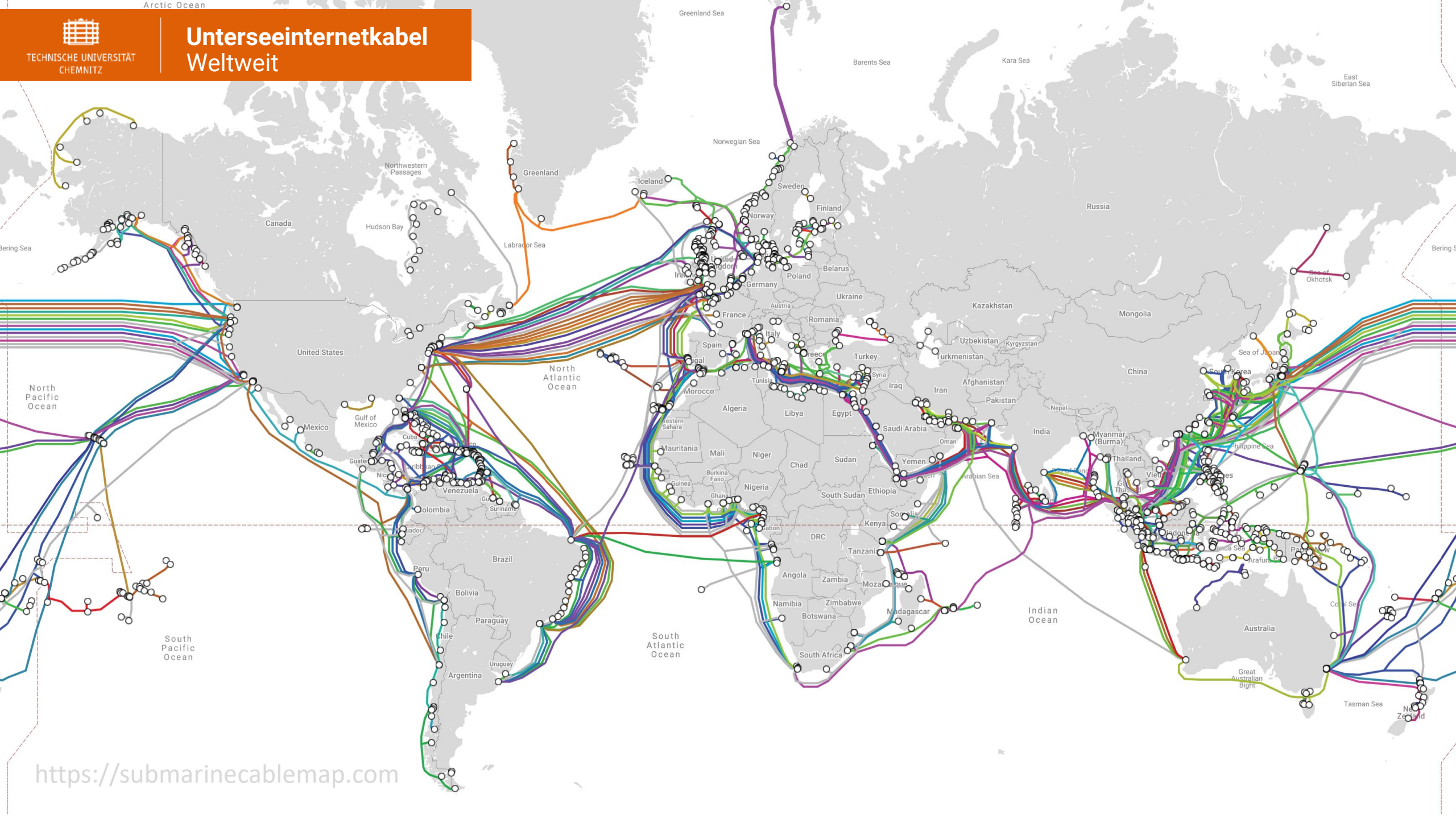


Der Prozentuale Anteil der Bevölkerung eines Landes, der das Internet nutzt

„Als Internetnutzer werden alle Personen gezählt, die das Internet in den letzten 3 Monaten genutzt haben.“

TECHNISCHE UNIVERSITÄT CHEMNITZ

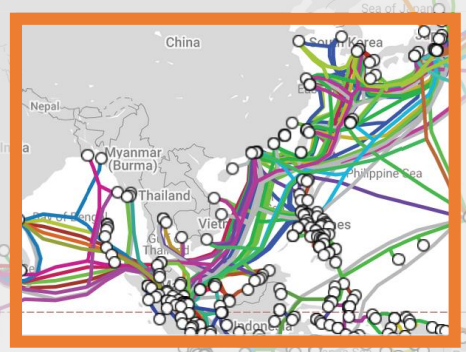
Unterseeinternetkabel
Weltweit



https://submarinecablemap.com

TECHNISCHE UNIVERSITÄT CHEMNITZ

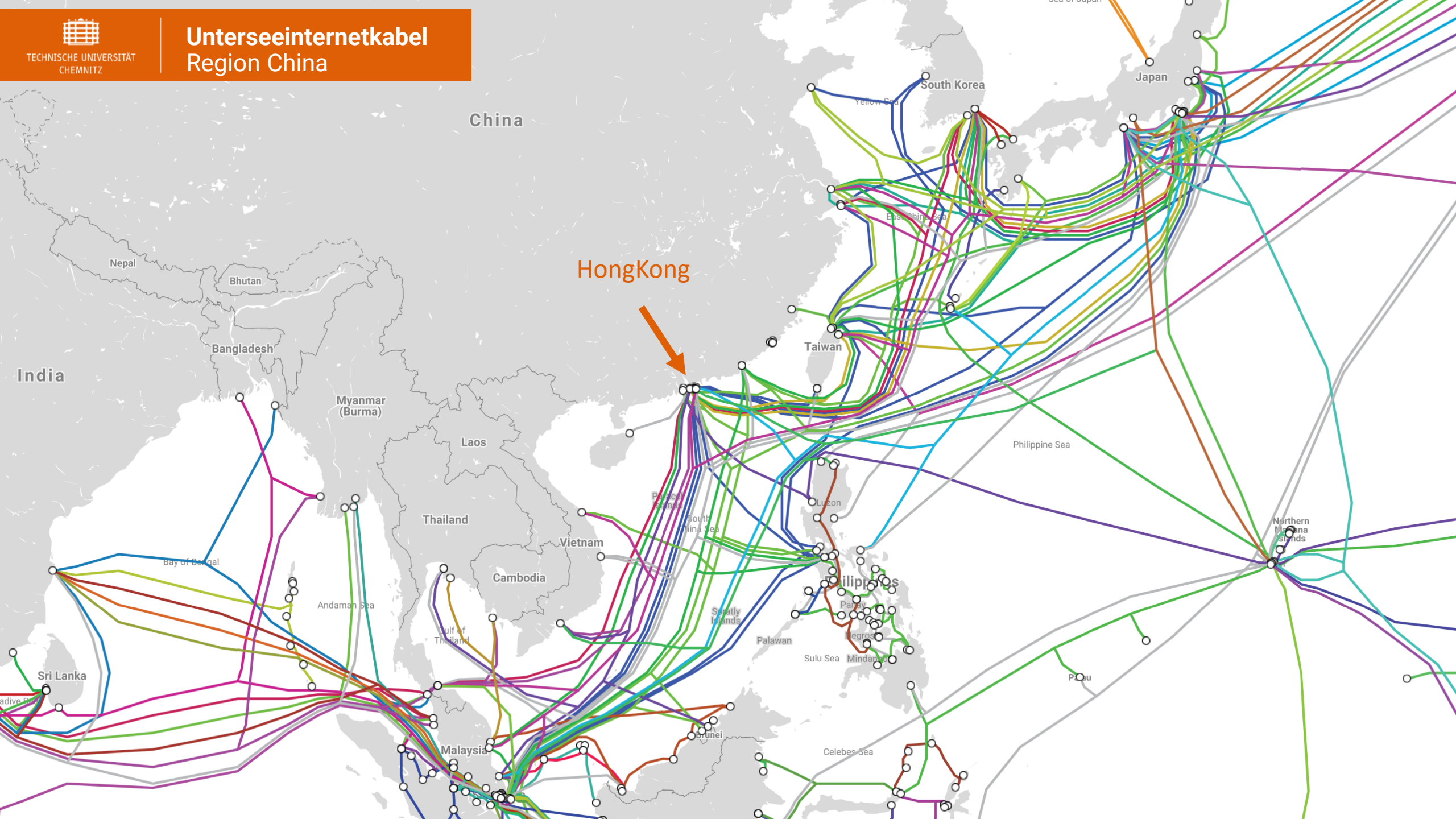
Unterseeinternetkabel
Weltweit



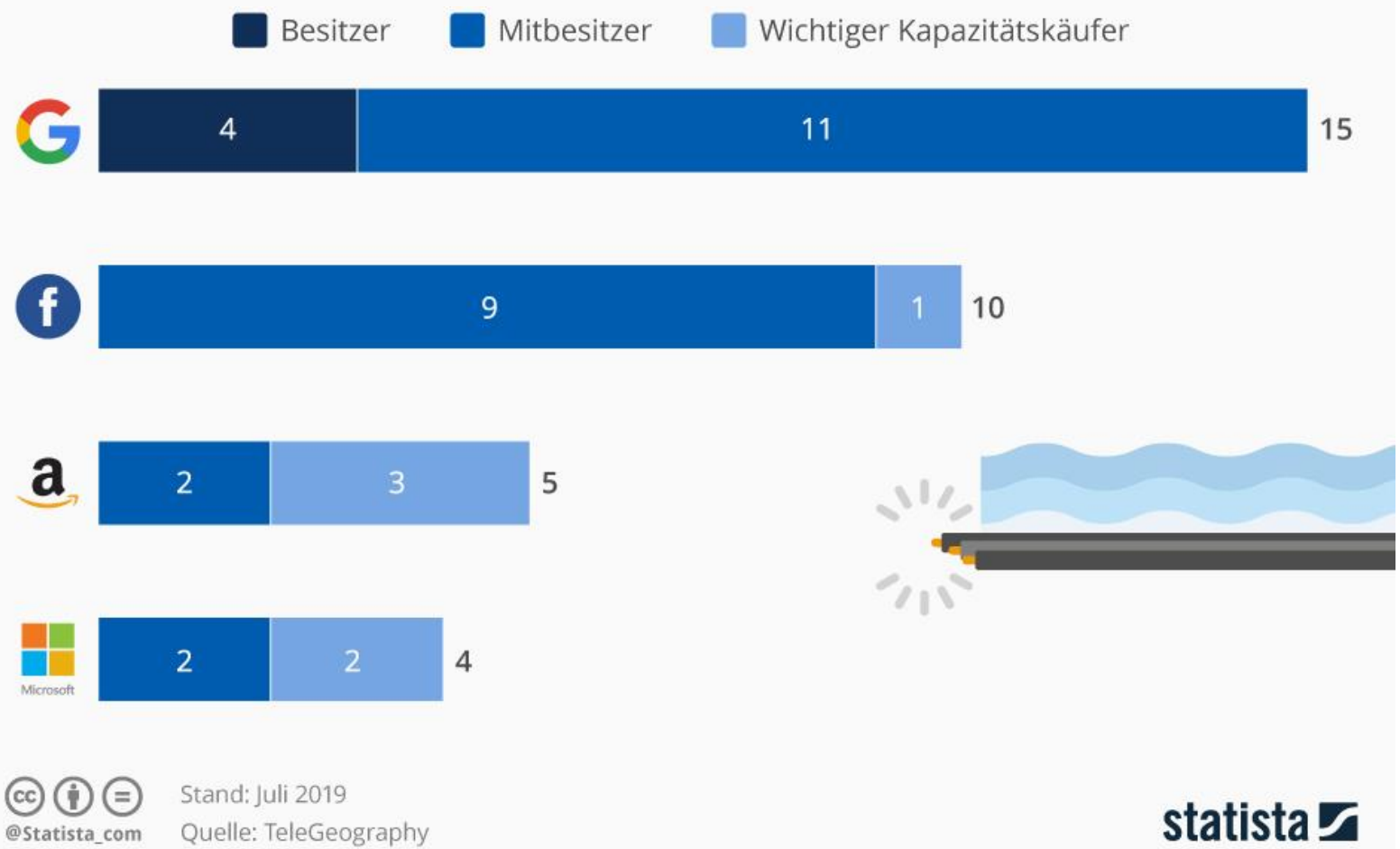
https://submarinecablemap.com

TECHNISCHE UNIVERSITÄT CHEMNITZ

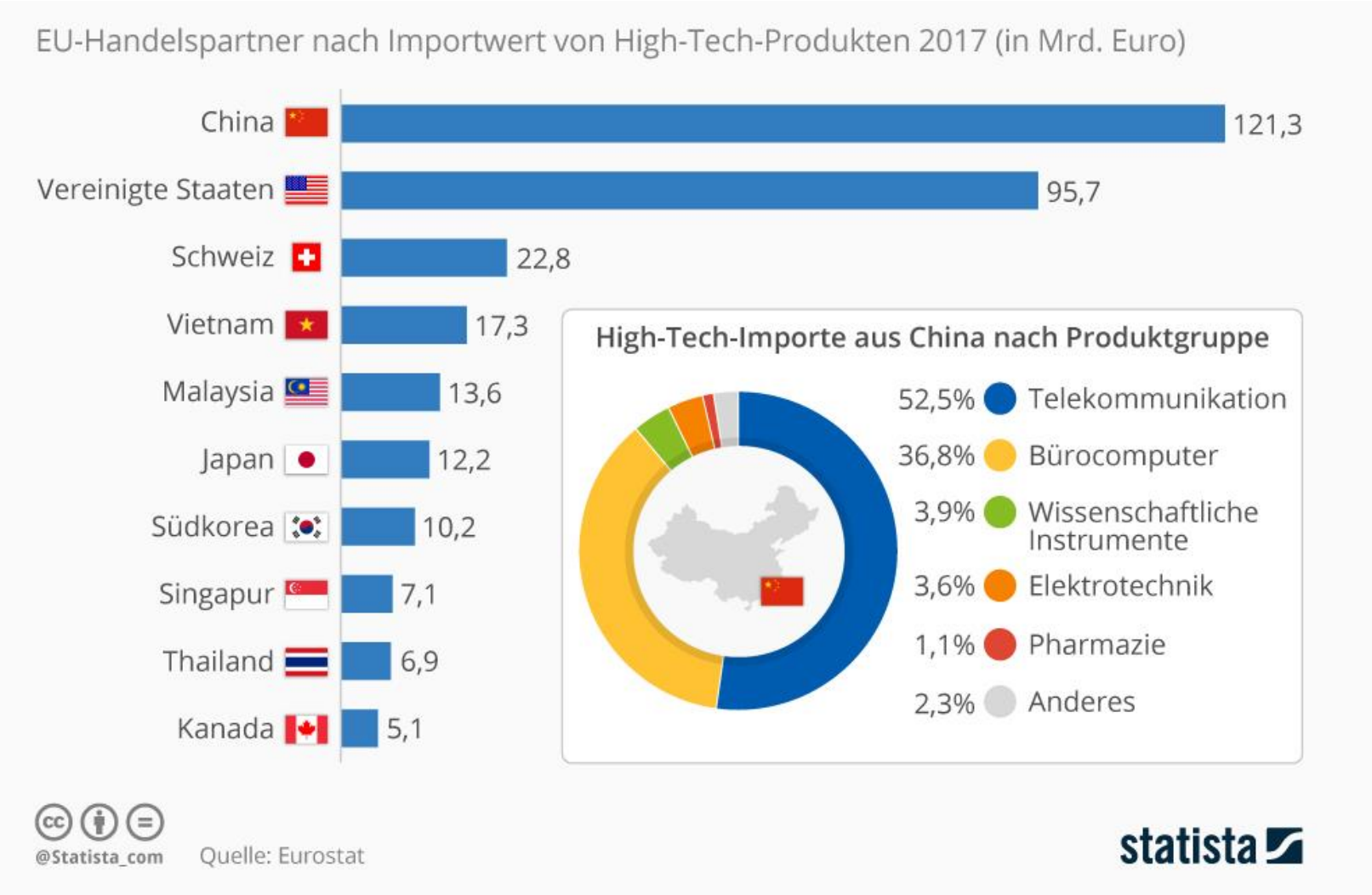
Unterseeinternetkabel
Region China



Unterwasser-Internetkabel mit direkter Beteiligung von Tech-Unternehmen



Woher die EU High-Tech bezieht



Fünf der Top 10 Größten Internetknotenpunkte befinden sich im Europäischen Raum, aber:

Die EU ist stark von China abhängig um diese Infrastruktur auf- und auszubauen.

Zentrale Datenansammlungen in fernen Datenräumen

Persönliche Daten

Transaktionsdaten

Metadaten

..liegen bei wenigen bei außereuropäischen Unternehmen

2 Formen von Cyberangriffen

[b: 4]

Hacktivismus

- nicht-profitorientiertes Nutzen von Hacking-Tools für Protest- bzw. Propagandazwecke
- Veröffentlichung gestohlener sensibler Daten mit ideologischem Hintergrund
- Gruppen: Anonymous, Cult of the Dead Cow
- Motivation häufig gegen Regierungen, Polizei, Konzerne
- Schäden häufig immaterieller Art

Cyberkriminalität

- Cyber-Attacken gegen Privatpersonen oder Unternehmen mit Ziel des persönlichen Profits
- Vielfältiger Mitteleinsatz
- Unterteilung in CCieS und CCiwS

Cyberspionage

- Nicht-profitorientierter Informationsraub öffentlicher Stellen
- Unterteilung in: Intrusiv und Nicht Intrusiv
- Russland, China, Iran meiste staatlich gestütze Cyberangriffe auf Deutschland
- Motivation ökonomischer, militärischer oder informeller Art

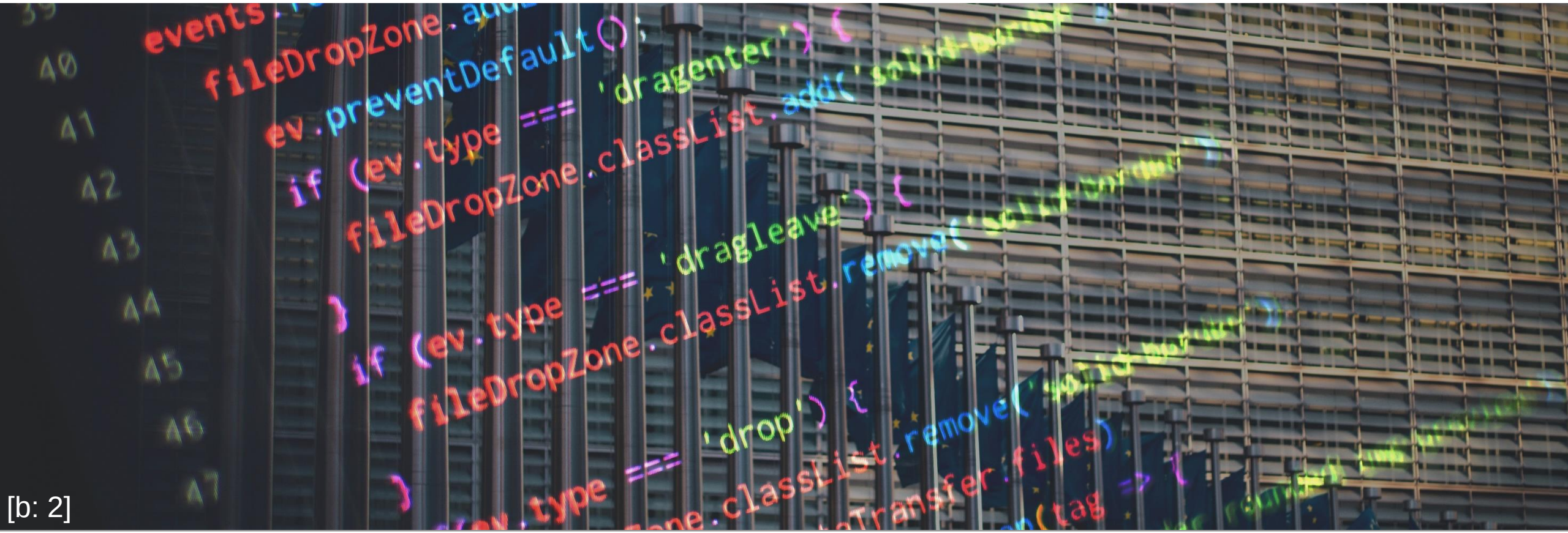
Cyberterrorismus

- Nutzen des Internets zu Propaganda- und Radikalisierungszwecken
- Ziel: Verursachen materielle oder physische Schäden

Cyberkrieg

- Cyber-Attacken zur Nutzung staatlicher Kriegsführung
- Ein Akteur muss eine Regierung sein
- Beispiel: Operation „Orchard“ 2007

3 Cyber-Außen- und Sicherheitspolitik der EU



[b: 2]

3.1 Akteure

	Frieden, Sicherheit, Justiz	*Binnenmarkt*	*GSVP: Cyberverteidigung*	*GASP: Cyberdiplomatie*
EU	Europol (EC3) Eurojust EU-LISA	ENISA CSIRT-Netzwerk CERT-EU	EDA GSA	EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM EU-Hybrid Fusion Cell ERCC
National	Exekutiv- und Datenschutzbehörden	Für die NIS zuständige Behörden Nationale CSIRTs	Verteidigungs-, Militär- und Sicherheitsbehörden	Außenministerien

3.2 Cyberdiplomatie

Vier Pfeiler EU-Cybersicherheit

1. Instrumente zur Täterverfolgung
2. IT-Infrastruktur sicherer gestalten, Verbraucherschutz / Nutzerinformation
3. Standardisierung Soldatensysteme
4. Bilaterale Cyberdialoge zwischen EU und Regierungen der Mitglieder

Diplomatischer Reaktionsrahmen

- Festlegung gemeinsamer diplomatischer Konsequenzen bei Angriff

Fünf Kategorien von Maßnahmen

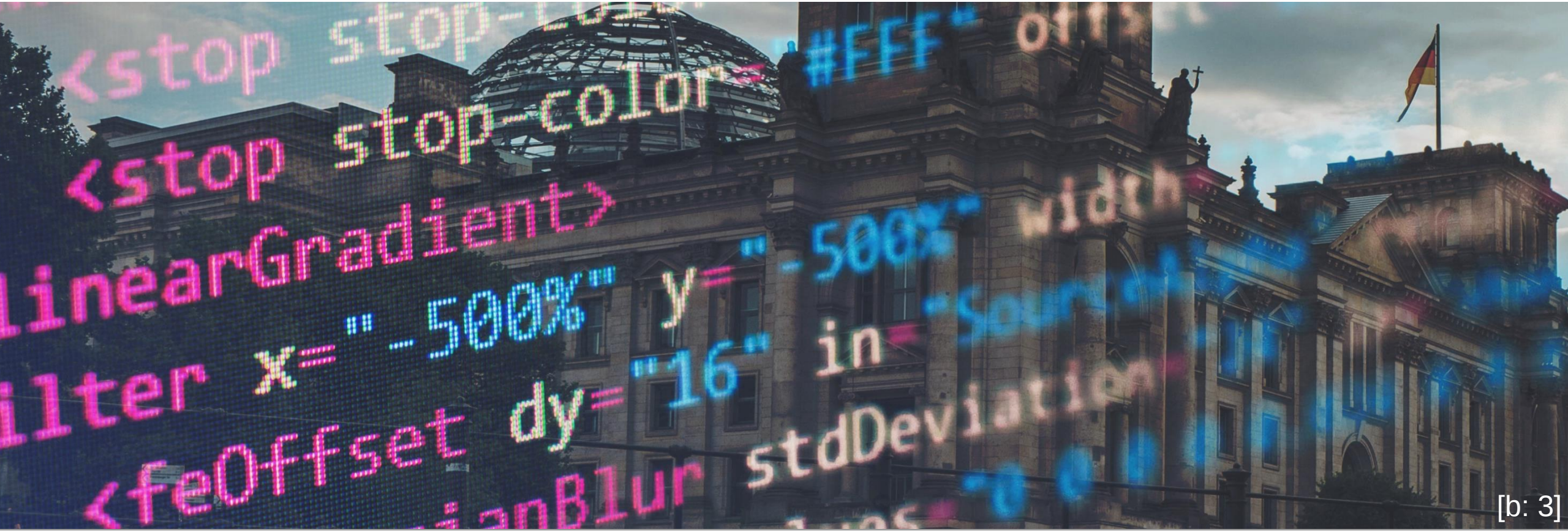
- Prävention
- Kooperation
- Stabilisierung
- Restriktionen
- Völkerrechtskonforme Reaktionen

Dual-Use Verordnung 2009

3.3 Probleme

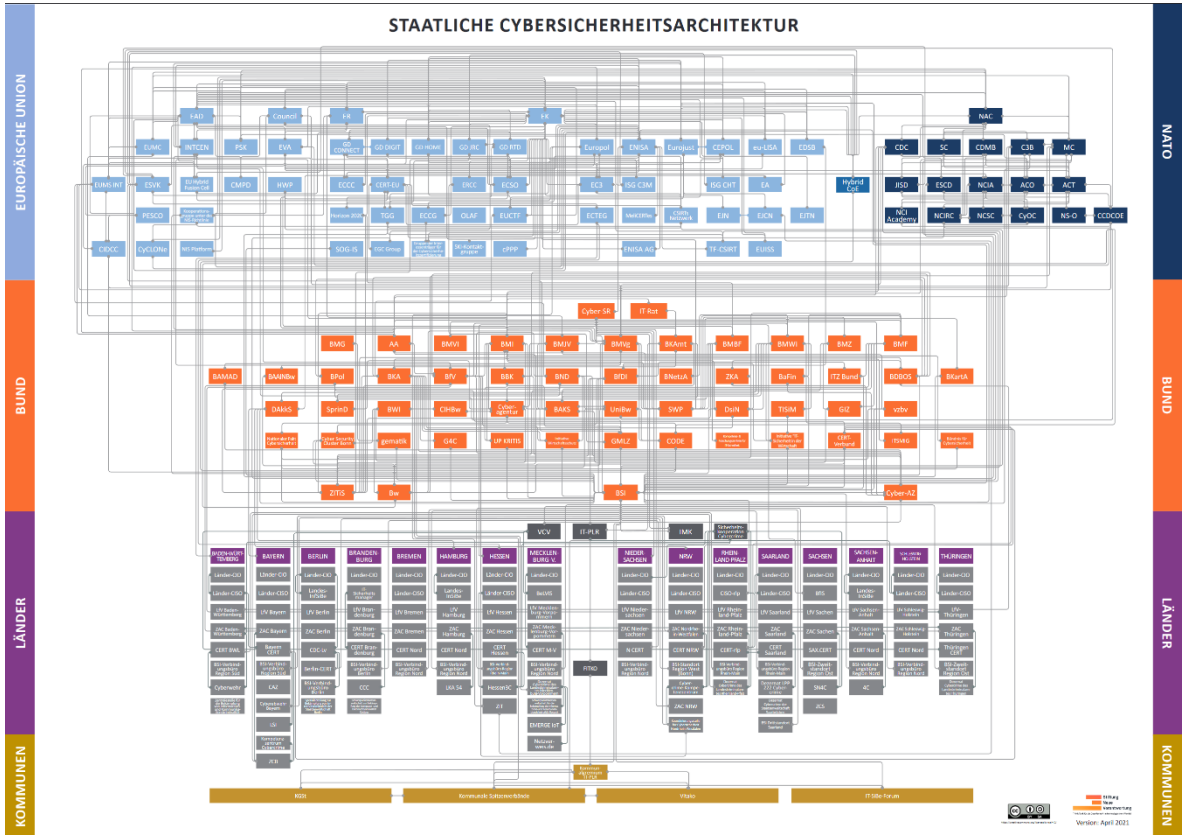
- Einstimmungszwang
  - →Verschiedene Interessen/Prioritäten der Mitgliedsstaaten
  - →Unterschiedliche technische Entwicklung der einzelnen Mitgliedsstaaten
- Mitgliedsstaaten müssen Anstrengungen zur Stärkung der Sicherheit im digitalen Rauem erhöhen
- Streitfrage wann aktive Verteidigung gerechtfertigt ist und wie die Kompetenzen verteilt werden
- Cyberdiplomatie nur wirksam, wenn sie europäische und globale Dimensionen mit einbezieht und geschlossen von allen Mitgliedsstaaten angewandt wird

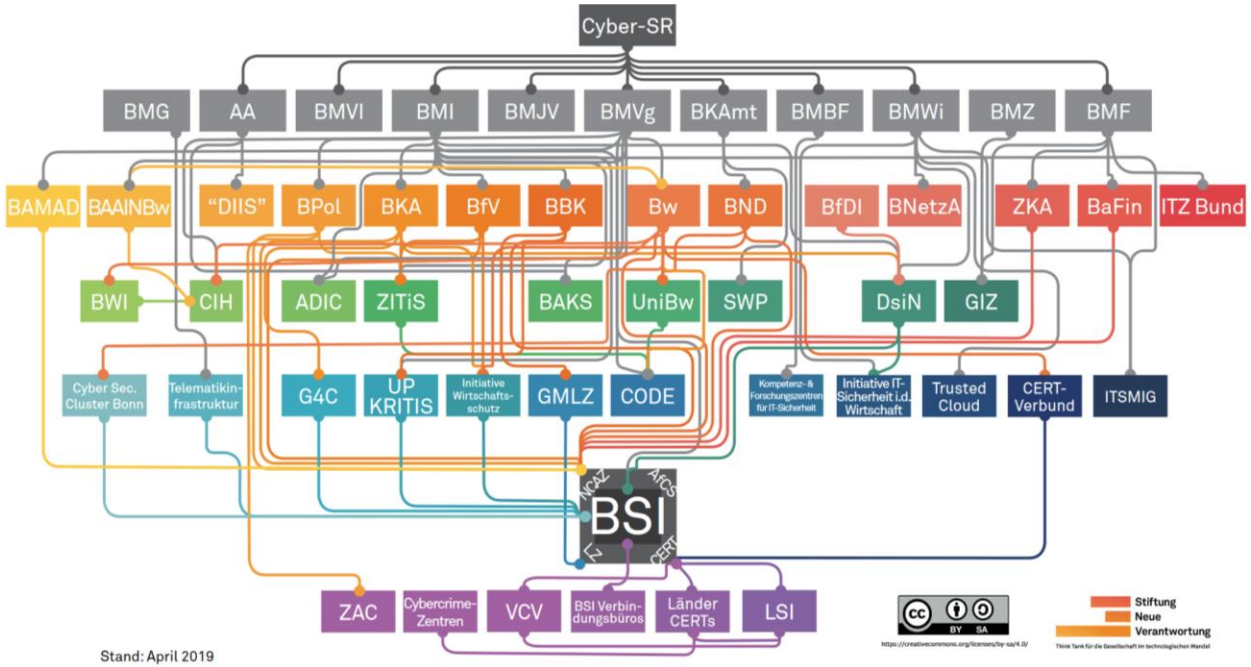
4 Deutsche Cybersicherheit

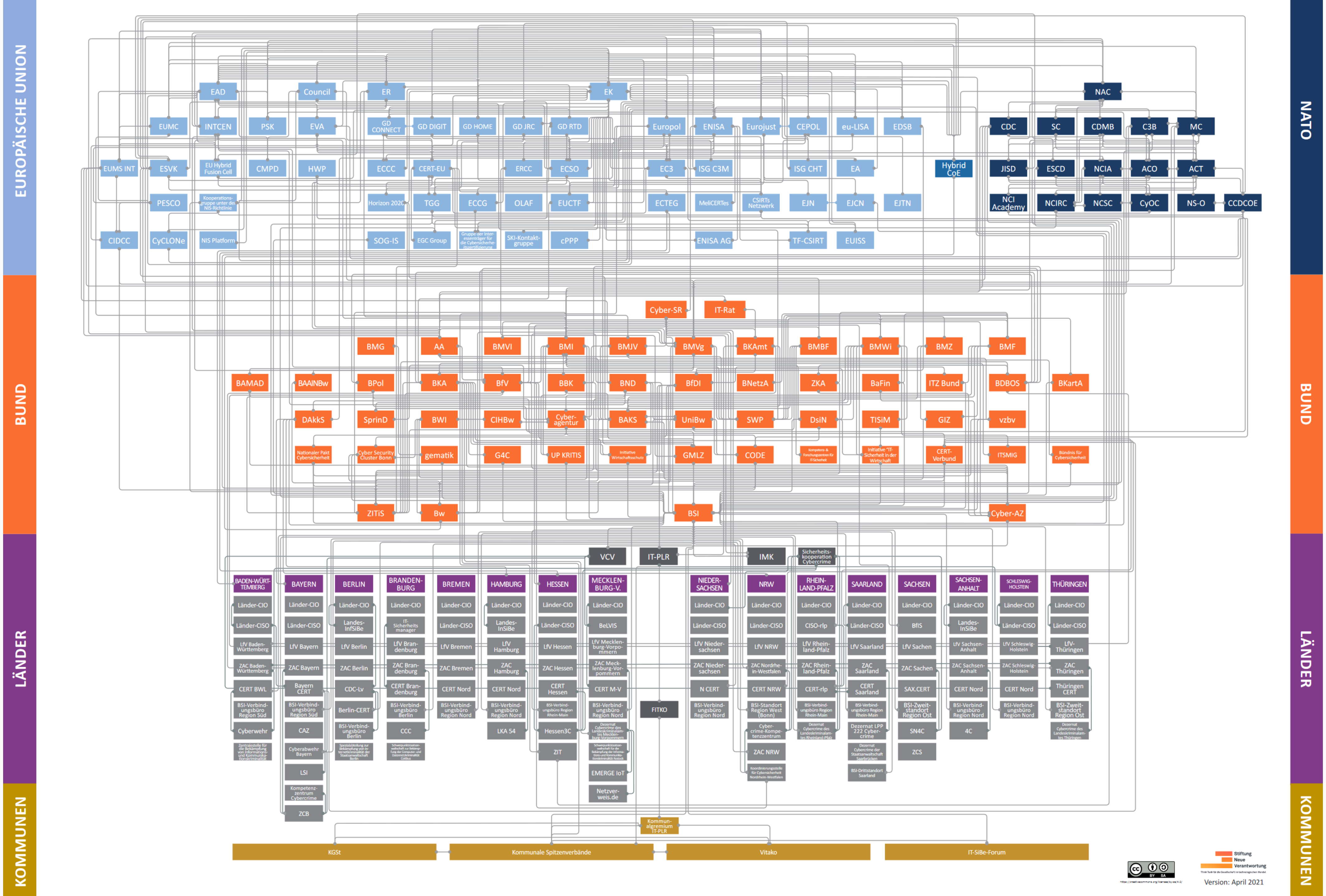


[b: 3]

4.1 Akteure

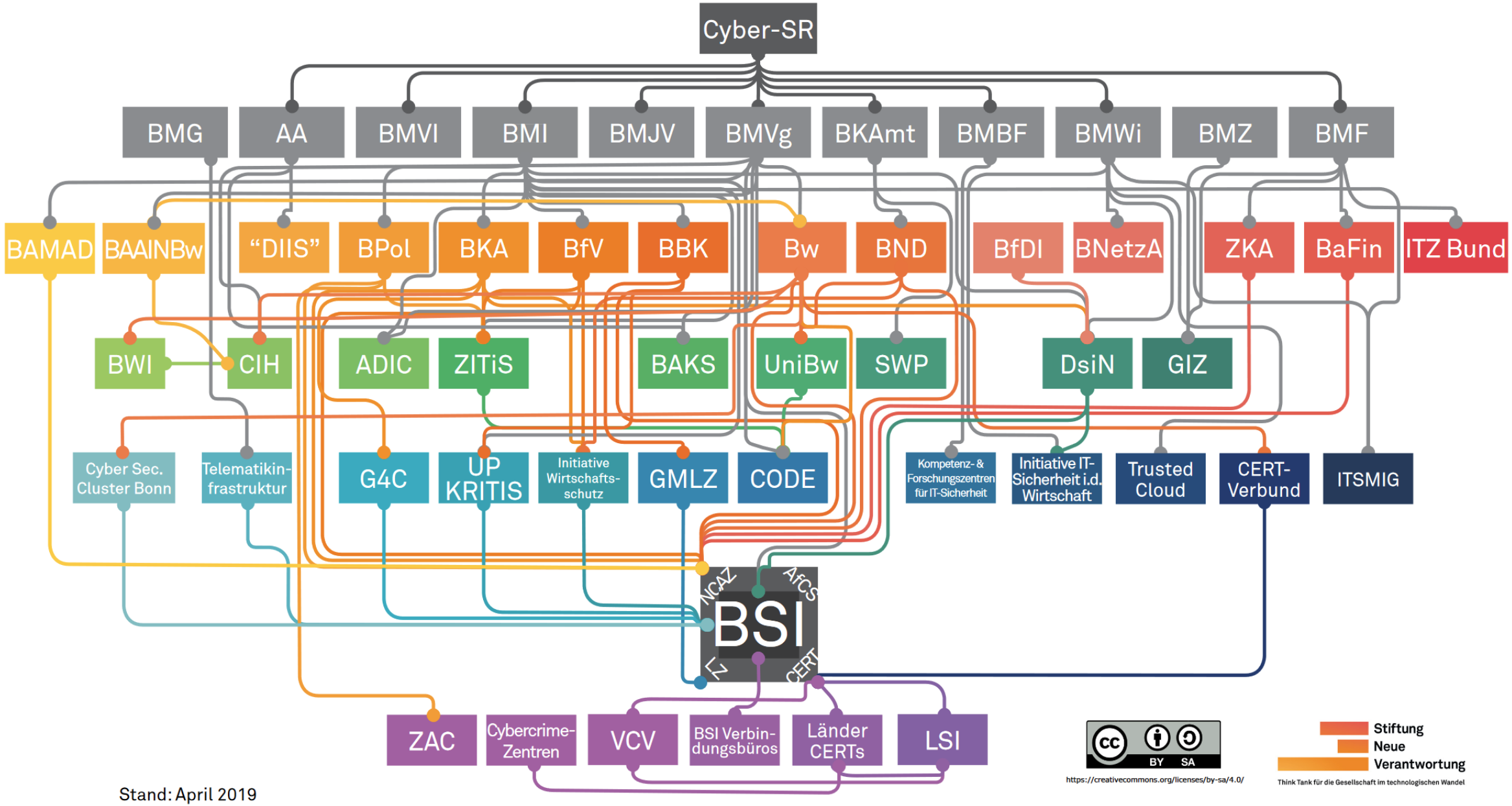

STAATLICHE CYBERSICHERHEITSARCHITEKTUR
EUROPÄISCHE UNION
BUND
LÄNDER
KOMMUNEN
NATO
BUND
LÄNDER
KOMMUNEN


Cyber-SR
BMG
AA
BMVI
BMI
BMJV
BMVg
BKAmt
BMBF
BMWi
BMZ
BMF
BAMAD
BAAINBw
"DIIS"
BPol
BKA
BfV
BBK
Bw
BND
BfDI
BNetzA
ZKA
BaFin
ITZ Bund
BWI
CIH
ADIC
ZITiS
BAKS
UniBw
SWP
DsiN
GIZ
Cyber Sec. Cluster Bonn
Telematikinfrastruktur
G4C
UP KRITIS
Initiative Wirtschaftsschutz
GMLZ
CODE
Kompetenz- & Forschungszentren für IT-Sicherheit
Initiative IT-Sicherheit i.d. Wirtschaft
Trusted Cloud
CERT-Verbund
ITSMIG
BSI
ZAC
Cybercrime-Zentren
VCV
BSI Verbindungsbüros
Länder CERTs
LSI
Stand: April 2019
Stiftung Neue Verantwortung



EUROPÄISCHE UNION
BUND
LÄNDER
KOMMUNEN
NATO
EAD
Council
ER
EK
EUMC
INTCEN
PSK
EVA
GD CONNECT
GD DIGIT
GD HOME
GD JRC
GD RTD
Europol
ENISA
Eurojust
CEPOL
eu-LISA
EDSB
EUMS INT
ESVK
EU Hybrid Fusion Cell
CMPD
HWP
ECCC
CERT-EU
ERCC
ECSO
EC3
ISG C3M
ISG CHT
EA
PESCO
Horizon 2020
TGG
ECCG
OLAF
EUCTF
ECTEG
MeliCERTes
CSIRTs Netzwerk
EJN
EJCN
EJTN
CIDCC
CyCLONe
NIS Platform
SOG-IS
EGC Group
SKI-Kontakt-gruppe
cPPP
ENISA AG
TF-CSIRT
EUISS
Hybrid CoE
NAC
CDC
SC
CDMB
C3B
MC
JISD
ESCD
NCIA
ACO
ACT
NCI Academy
NCIRC
NCSC
CyOC
NS-O
CCDCOE
Cyber-SR
IT-Rat
BMG
AA
BMVI
BMI
BMJV
BMVg
BKAmt
BMBF
BMWi
BMZ
BMF
BAMAD
BAAINBw
BPol
BKA
BfV
BBK
BND
BfDI
BNetzA
ZKA
BaFin
ITZ Bund
BDBOS
BKartA
DAkkS
SprinD
BWI
CIHBw
Cyber-agentur
BAKS
UniBw
SWP
DsiN
TISiM
GIZ
vzbv
Nationaler Pakt Cybersicherheit
Cyber Security Cluster Bonn
gematik
G4C
UP KRITIS
Initiative Wirtschaftsschutz
GMLZ
CODE
Initiative "IT-Sicherheit in der Wirtschaft"
CERT-Verbund
ITSMIG
Bündnis für Cybersicherheit
ZITiS
Bw
BSI
Cyber-AZ
VCV
IT-PLR
IMK
Sicherheits-kooperation Cybercrime
BADEN-WÜRTTEMBERG
BAYERN
BERLIN
BRANDEN-BURG
BREMEN
HAMBURG
HESSEN
MECKLEN-BURG-V.
NIEDER-SACHSEN
NRW
RHEIN-LAND-PFALZ
SAARLAND
SACHSEN
SACHSEN-ANHALT
SCHLESWIG-HOLSTEIN
THÜRINGEN
Länder-CIO
Länder-CISO
Landes-InfSiBe
IT-Sicherheits-manager
BeLVIS
CISO-rlp
BfIS
LfV Baden-Württemberg
LfV Bayern
LfV Berlin
LfV Bran-denburg
LfV Bremen
LfV Hamburg
LfV Hessen
LfV Mecklen-burg-Vorpo-mmern
LfV Nieder-sachsen
LfV NRW
LfV Rhein-land-Pfalz
LfV Saarland
LfV Sachen
LfV Sachsen-Anhalt
LfV Schleswig-Holstein
LfV-Thüringen
ZAC Baden-Württemberg
ZAC Bayern
ZAC Berlin
ZAC Bran-denburg
ZAC Bremen
ZAC Hamburg
ZAC Hessen
ZAC Meck-lenburg-Vor-pommern
ZAC Nieder-sachsen
ZAC Nordrhe-in-Westfalen
ZAC Rhein-land-Pfalz
ZAC Saarland
ZAC Sachen
ZAC Sachsen-Anhalt
ZAC Schleswig-Holstein
ZAC Thüringen
CERT BWL
Bayern CERT
CDC-Lv
CERT Bran-denburg
CERT Nord
CERT Hessen
CERT M-V
N CERT
CERT NRW
CERT-rlp
CERT Saarland
SAX.CERT
Thüringen CERT
Cyberwehr
CAZ
Berlin-CERT
CCC
LKA 54
Hessen3C
ZIT
EMERGE IoT
Netzver-weis.de
FITKO
Cyber-crime-Kompe-tenzzentrum
ZAC NRW
SN4C
ZCS
4C
Cyberabwehr Bayern
LSI
Kompetenz-zentrum Cybercrime
ZCB
Dezernat LPP 222 Cyber-crime
Kommun-algremium IT-PLR
KGSt
Kommunale Spitzenverbände
Vitako
IT-SiBe-Forum
Stiftung Neue Verantwortung
Version: April 2021

Staatliche Cybersicherheitsarchitektur



Stand: April 2019

Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel

4.1 Akteure

- Cyber-Sicherheitsrat
- BSI (Bundesamt für Sicherheit in der Informationstechnik)
- BND (Bundesnachichtendienst)
- Bundeswehr
- ZITiS (Zentrale Stelle für Informationstechnik im Sicherheitsbereich)
- CERT (Computer Emergency Response Team)

4.2 Cyberkriminalität in Deutschland

- Täter höchst professionell, arbeitsteilig, global vernetzt und international agierend
- Ransomware größte Gefahr für deutsche Unternehmen
- Anstieg CCieS um 15,4% auf ca. 100.500 Fälle (2019)
- 579 OK-Verfahren 2019 (2018: 13 verfahren)
- 87,7 Mio. Euro Schaden durch Computerbetrug (+44,4%)

4.3 Probleme

- Deutschland Teil Amerikanisch-Chinesischen Oligopols
  - →Wesentliche Infrastrukturen und Dienstleistungen von außereuropäischen Anbietern bereitgestellt
  - →Wenige große Akteure (Amazon, Microsoft, Apple, Huawei, Alibaba)
- Unvollendeter digitaler Binnenmarkt
- Vorwiegend regulatorische Reaktionen auf digitale Bedrohungen
- Zu viele Akteure die an Deutscher Cybersicherheitspolitik beteiligt sind
- Bundeswehr nicht für digitale Kriegsführung gerüstet

4.3 Mögliche Lösungsansätze

- Reduzierung Behörden, mehr Kompetenzen für bestehende

  → z.B. Aufbau eigenes Ministerium
- Offensive Gegenreaktionen (z.B. Hackbacks) als Maßnahme erleichtern
- Stärkere Investition in konkurrenzfähige IT-Unternehmen
- Schaffung gemeinsamer Datennetze/-zentren auf europäischer Ebene

  →Deutschland Schlüsselrolle in EU

  →Behauptung Werte der EU im digitalen Raum ermöglicht durch Kontrolle eigener Datennetze

4.3 Mögliche Lösungsansätze

- Abhängigkeit von geschlossenen Systemen reduzieren
  - → Auf gemeinsame, offene Software setzen
  - → Qualität von Open-Source-Software sicherstellen
- Defensive Sicherheitsmaßnahmen ausbauen
  - → Dezentrale statt zentrale Systeme
  - → Ende-zu-Ende-Verschlüsselung zum Standard machen
- Wirken von Geheimdiensten einschränken
  - → Unabhängige und evidenzbasierte Sicherheits- und Geheimdienstpolitik

Bildquellen [b : n]

1. https://unsplash.com/photos/8bghKxNU1j0
2. https://unsplash.com/photos/MZWBMNP7Nro + https://unsplash.com/photos/_SgRNwAVNKw
3. https://unsplash.com/photos/dmtOsXvl8jc + https://unsplash.com/photos/4hbJ-eymZ1o
4. https://unsplash.com/photos/RlLP5fUh2m0

Weiterführends

- **Verein:** Chaos Computer Club (DE + EU)
- **Blog:** Netzpolitik.org (DE + EU)
- **Podcast:** Logbuch Netzpolitik (eher DE)
- **Verein:** Digitalcourage (DE)

Diskussion: Statement

Die Sicherheit von (allen) IT-Systemen sollte über den Hack-befugnissen von Geheimdiensten und Behörden stehen.

Diskussion: Statement

Die EU sollte ein eigenes Google aufbauen, um sich unabhängig von ausländischen Tech-Giganten zu machen.