CROSSING Conference 2023

TU Darmstadt

Manuel ‚HonkHase‘ Atug

Critical Infrastructure Security

Manuel ‚HonkHase‘ Atug

Manuel ‘HonkHase’ Atug

Principal at HiSolutions AG

- Graduate computer scientist, Master of Science in Applied IT Security, Engineer
- Expert for e.g. the IT-SiG 2.0 (critical infrastructure law) hearing at German Bundestag
- Topics: KRITIS, Hackback, Ethics, Hybrid Warfare, Cyberresilience, Civil protection and disaster control

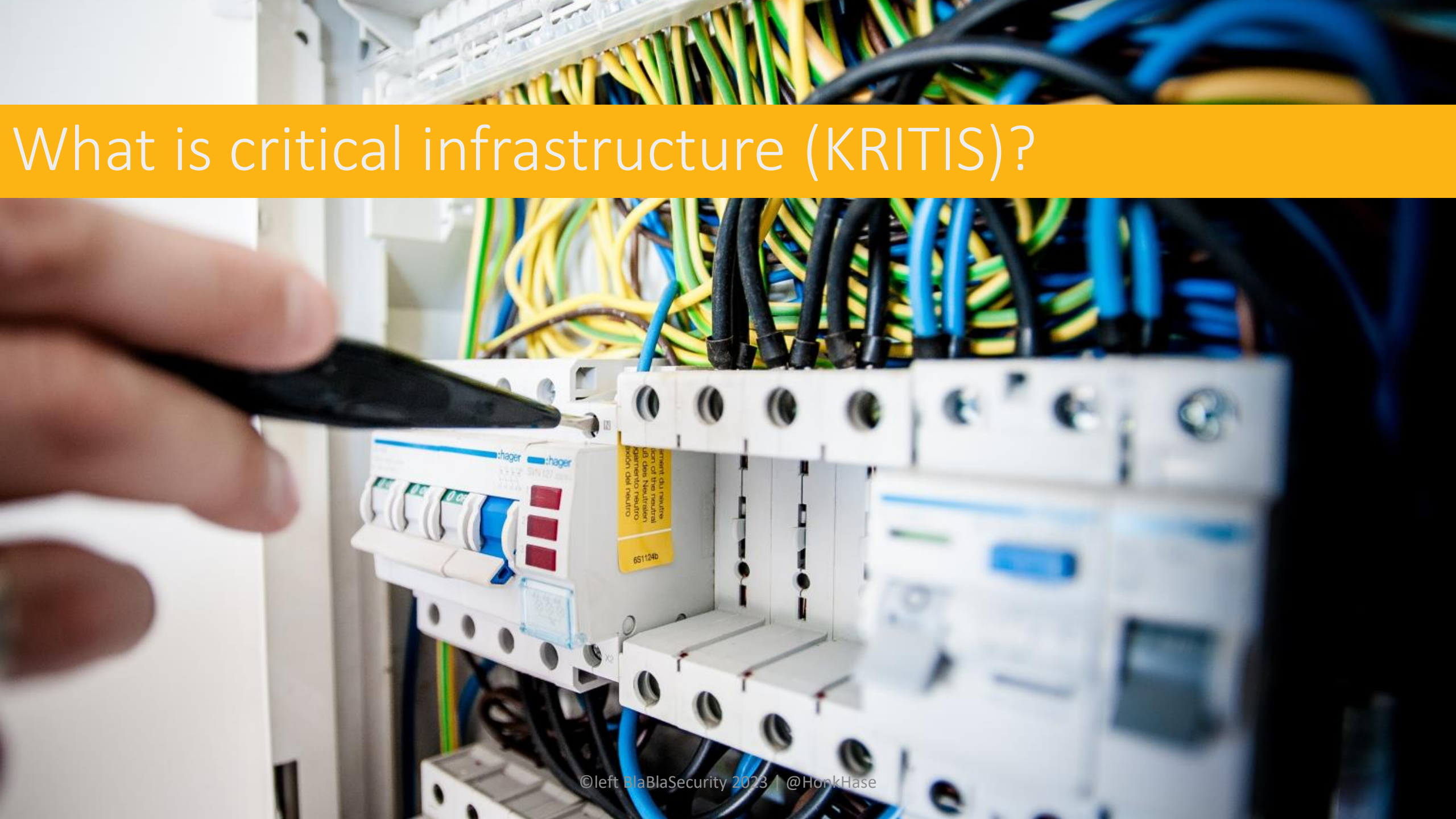
- Co-founder of AG KRITIS: ag.kritis.info

- Co-founder of AGND: www.agnd.eu

@HonkHase @HonkHase@chaos.social

I have #KRITIS in the final stage

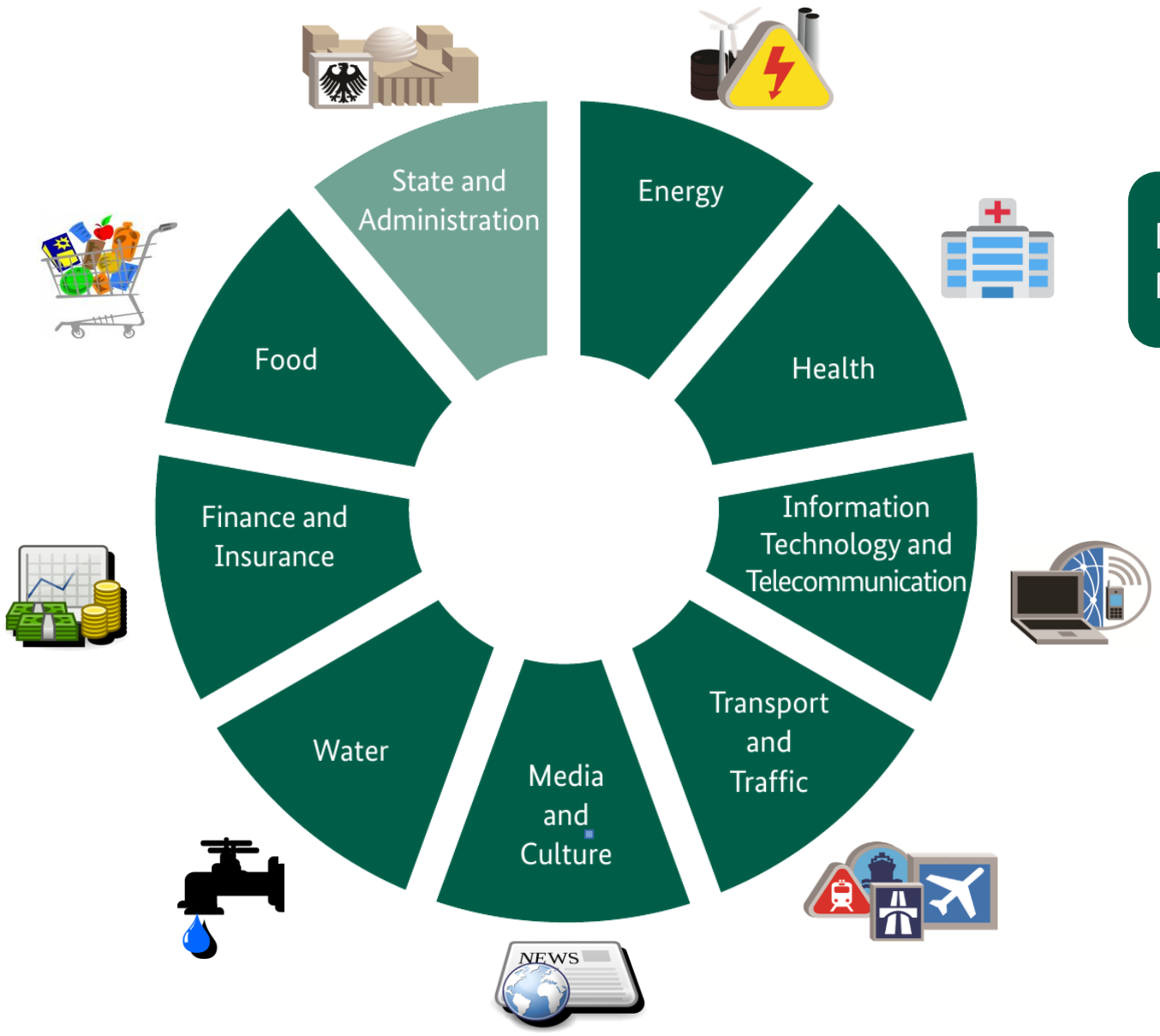
What is critical infrastructure (KRITIS)?



Definition of a critical infrastructure (KRITIS)

Critical infrastructures *are organizational and physical structures and facilities of such* ***vital importance*** *to a* ***nation's society and economy*** *that their* ***failure or degradation*** *would result in* ***sustained supply shortages****, significant* ***disruption of public safety and security****, or other* ***dramatic consequences***

Critical infrastructures in Germany



New via IT-Security law 2.0:
Municipal waste management

Source: BSI

Quo vadis KRITIS?

- Primarily protection of the population (not the operator)
- Often contains identical components
- More and more components are connected to the Internet
- OT is in operation for decades!

Cyberspace results in risks for everyone

Being KRITIS results in higher risks

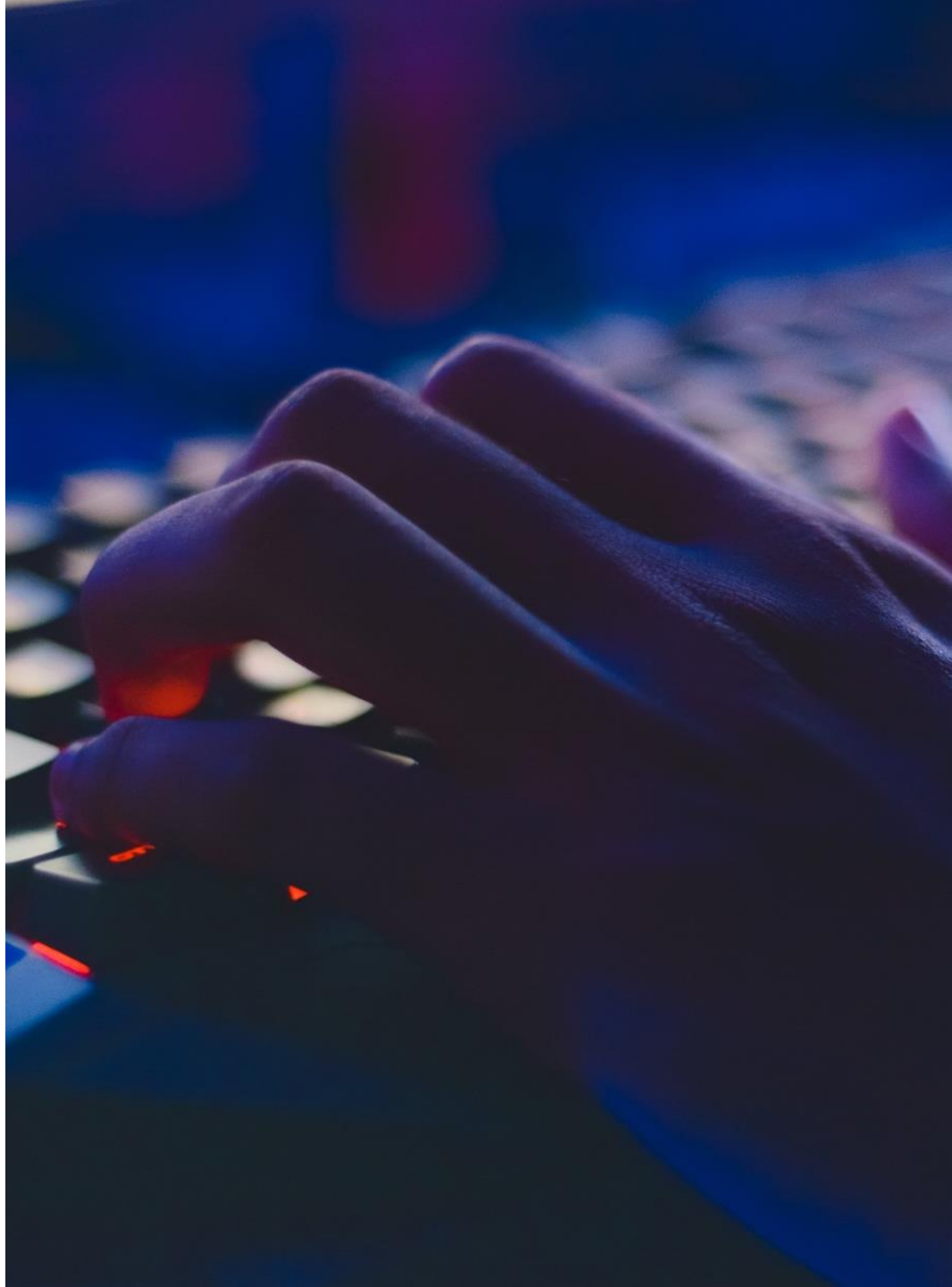
Higher risks are higher

Supply-Chain attack

- Cyberattack to a company by exploiting vulnerabilities via its service providers, managed services providers or via remote access
- E. g. Kaseya, SolarWinds, Kisters AG…

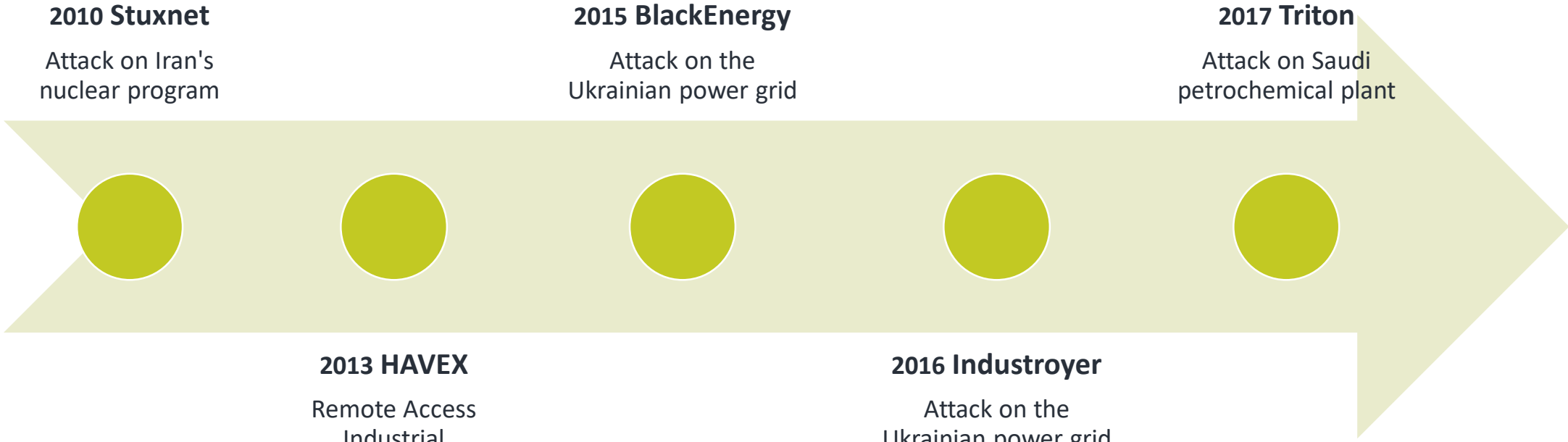
Ransomware

- Cyberattack to a company by encrypting the victim's data and threaten to publish data until a ransom is paid
- E. g. Emotet, WannaCry, NotPetya, Ryuk, GrandCrab, Maze, Conti, Revil, DoppelPaymer…



cyber-physical attacks

Timeline of ICS attacks



Again: Higher risks are higher

Threats become bigger

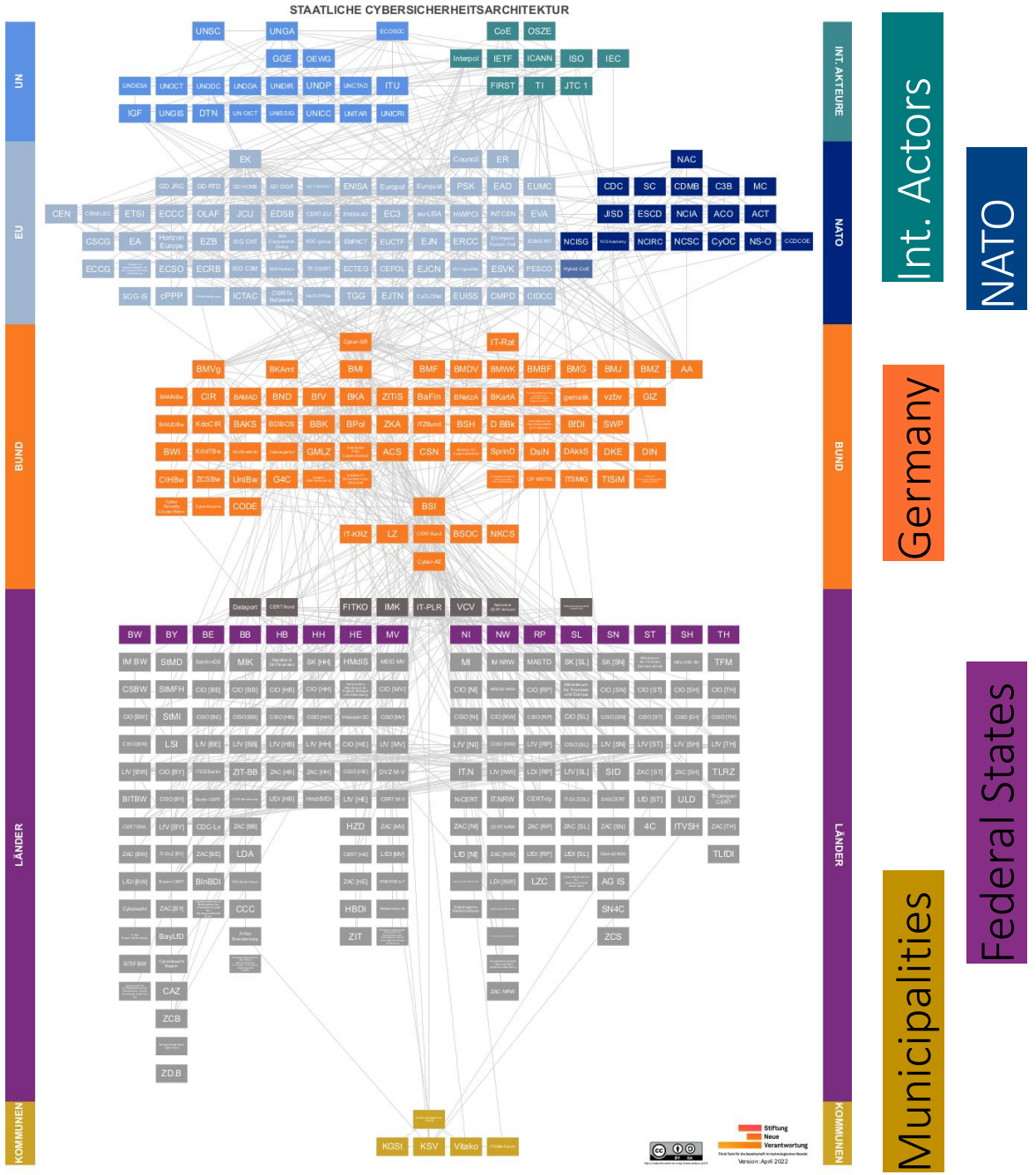
- hybrid warfare (also collateral damage!)
- Organized Cybercrime
- IT dependency
- „Cyber-Hooligans“
- Digitalization & globalization
- IP'ification of all the things

And it gets worse and worse :-(

- <here shall be positive news>

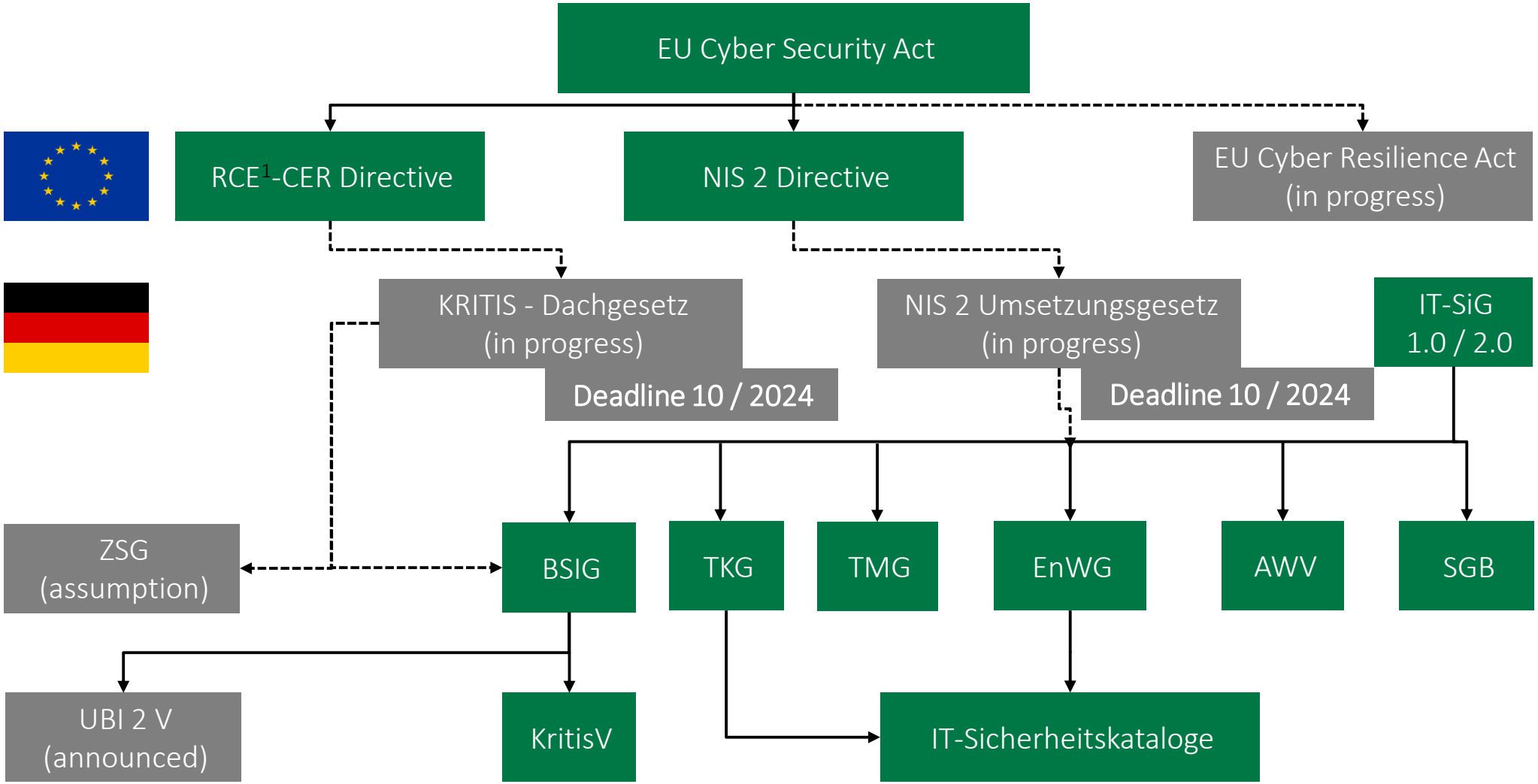
Help is comming!

Errr… wait O_o



Solutions anyone?

Overview of the regulatory structure (EU/DE)



>> all-dangers-approach <<

„Consideration of all types of possible danger in the context of risk- and crisis management “

** Hi Federal Office for Civil Protection*

Cyberresilience ➔ Resistance to events

- Cause of disaster or cyber incident is not relevant to the population
- But: a crisis (pandemic) in crisis (Putin's war of aggression) in crisis (ransomware) in crisis (gas shortage) in <insert any crisis here> nobody needs!
- Critical questions:

  → Is digitalization always necessary?

  →Can we use it to increase cyber resilience?

  →What is good digitalization?

Sustainability in digitalization

- Initiating responsible measures in digital transformations and implementing them conscientiously, i.e. operationalizing them, is therefore both a technical and an ethical task!
- Therefore avoid technical debt to future generations
- Behind every data set is a human being ➔ Data is toxic
- Security by Design and Privacy by Design is Human Protection

And what do I do if all else fails?

Something with wood?

Coconut picker!

www.kokosnusspflücker.de