HISOLUTIONS

Critical Infrastructure (KRITIS) in Cyberspace
Complex and Dangerous?

DeepSec 2021

Manuel Atug

About me

Manuel Atug

- Head of Business Development at HiSolutions AG
- Computer scientist, M. Sc. in Applied IT Security, Engineer
- > 23 years of experience in information security
- Many years of experience in the field of technical IT-Sec and audits
- Topics: critical infrastructure, hackback, ethics, civil protection

@HonkHase

Security Consulting Service Portfolio

Penetration tests/ technical audits

Cyber response/ forensics

ISMS ISO

ISMS Grundschutz

Privacy/ Data Protection

Auditing/ Certification

Awareness and Training

Business Continuity

Crisis management

IT emergency management

concepts/ Risk Analysis

Emergency and crisis exercises

Outsourcing

Cloud Security

Wirtschaftsgrundschutz

Corporate security

Security strategy

Industrial security

Medical security

Critical infrastructures

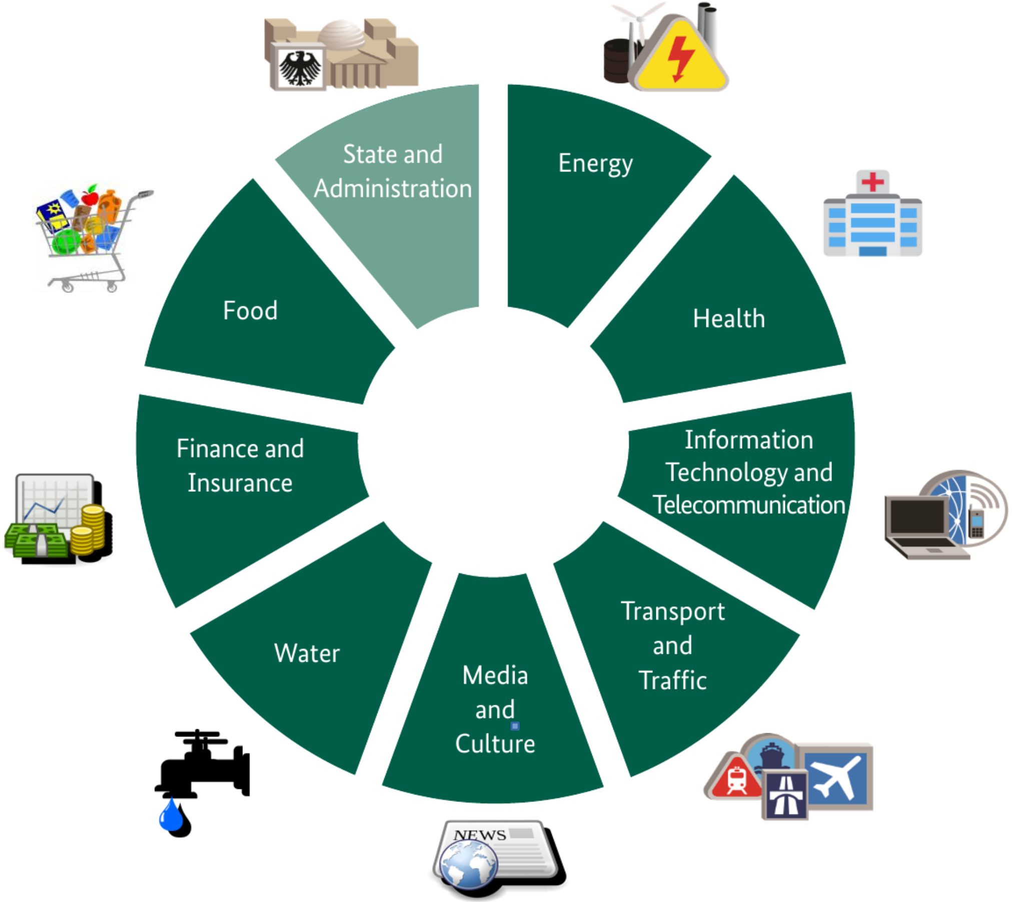
Risk management

Definition of a critical infrastructure

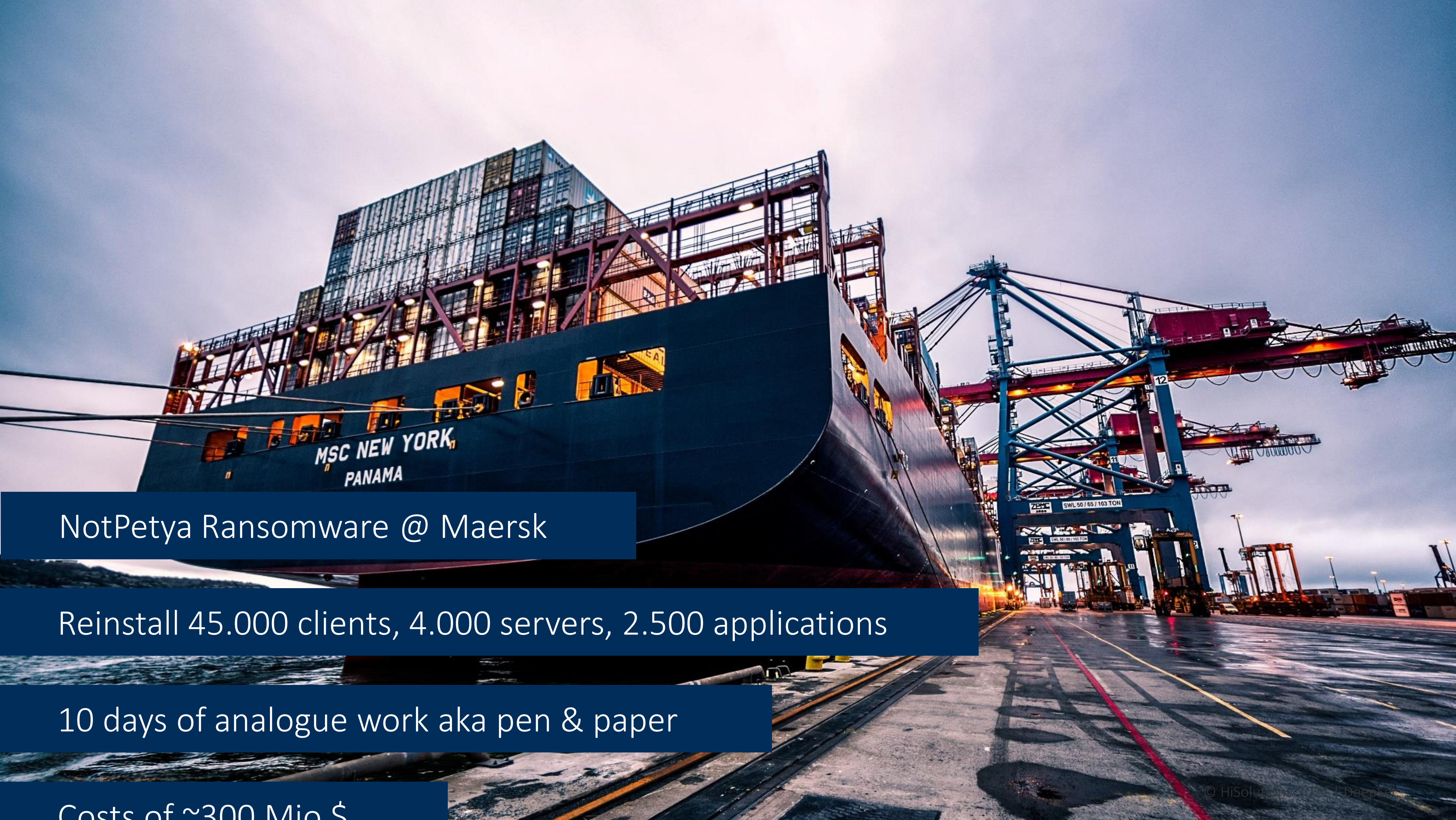
Definition of a critical infrastructure (KRITIS)

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 German IT-Security Law 2.0: Municipal Waste Disposal



NotPetya Ransomware @ Maersk

Reinstall 45.000 clients, 4.000 servers, 2.500 applications

10 days of analogue work aka pen & paper

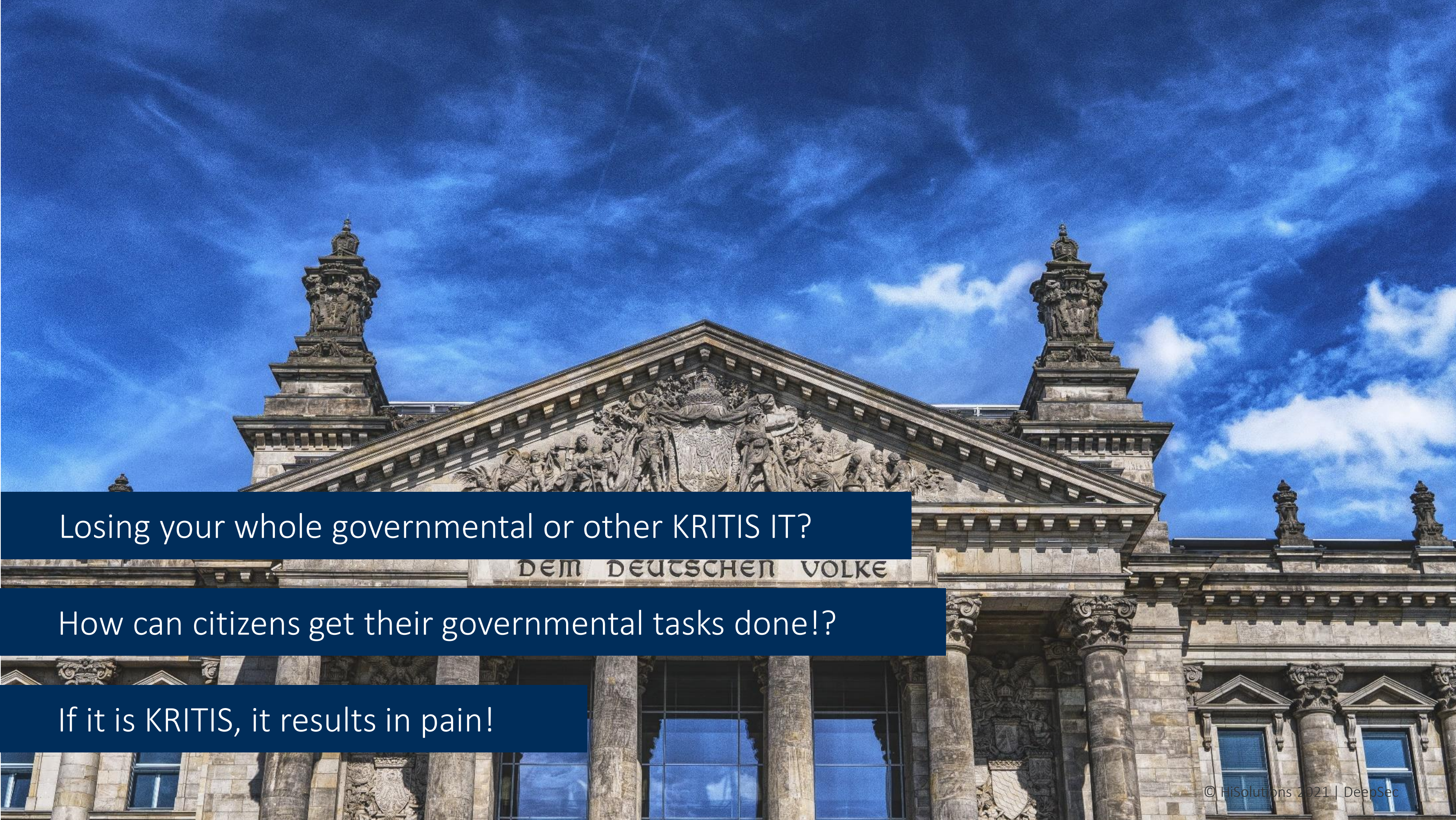
Costs of ~300 Mio $

Petya Ransomware @ TNT Express

Computer systems severely disrupted, deliveries and sales continued to suffer

Fully restore all its IT operations

Costs of ~300 Mio $

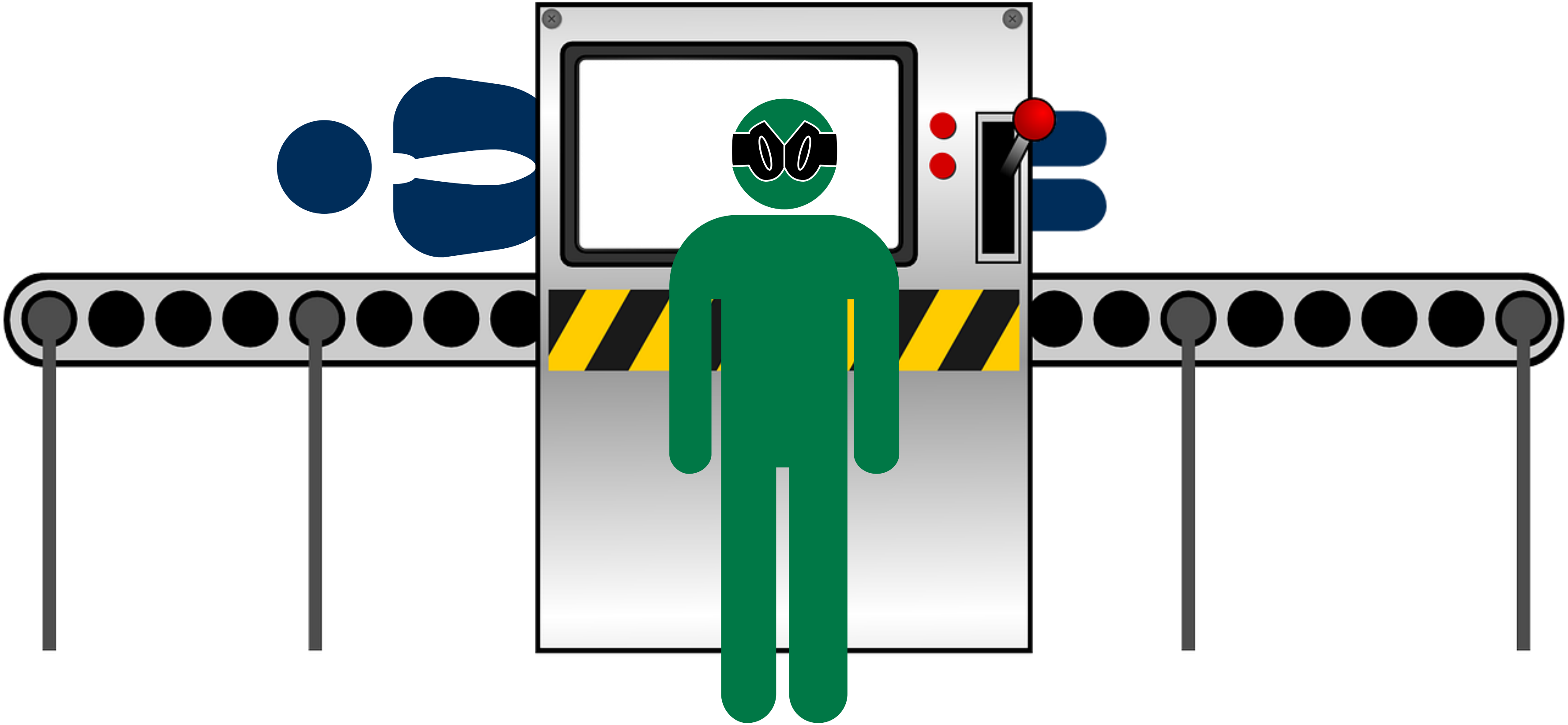


Losing your whole governmental or other KRITIS IT?

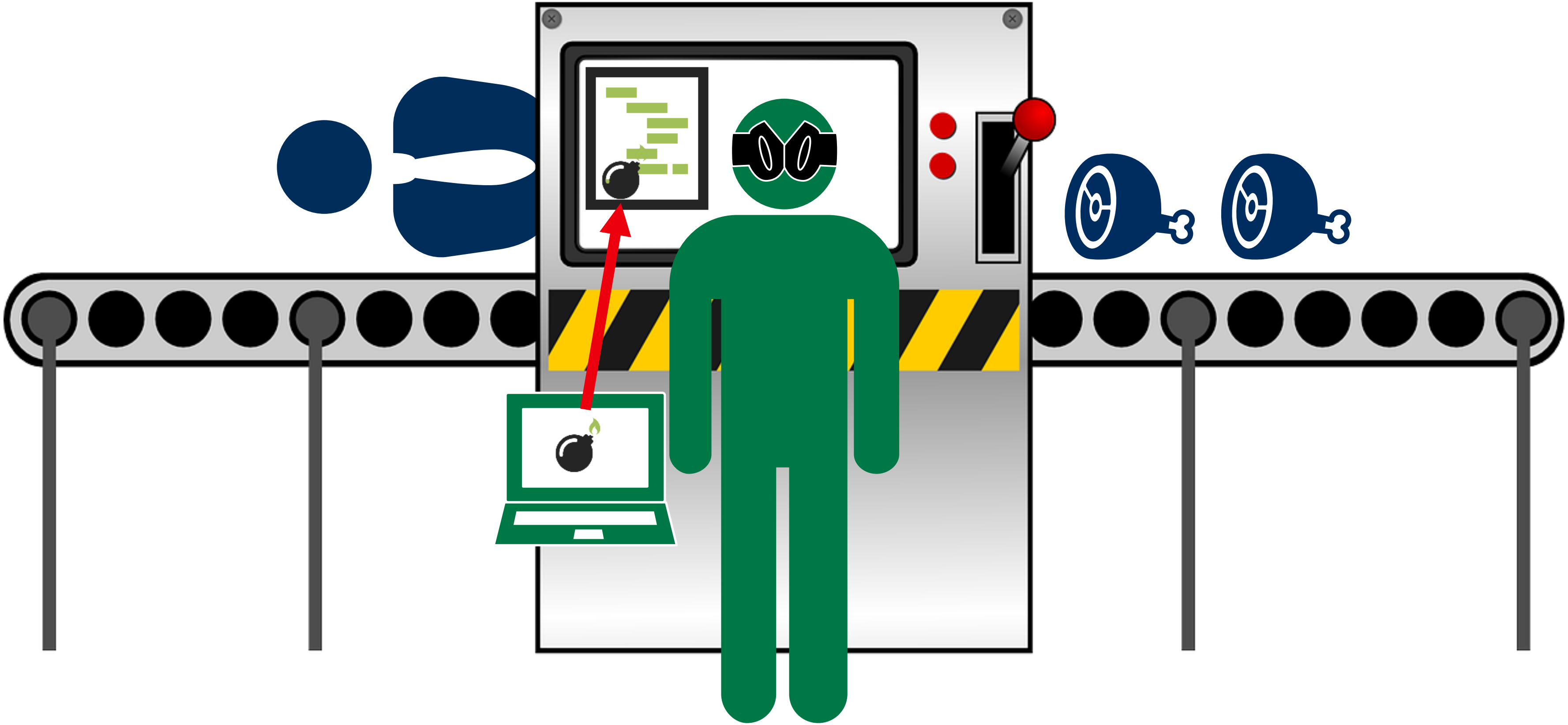
How can citizens get their governmental tasks done!?

If it is KRITIS, it results in pain!

Safety vs Security – Safety point of view: old style mechanical OT



Safety vs Security – Security point of view: new style IT (in OT!)



Cyberspace results in risks for everyone

Being KRITIS results in higher risks

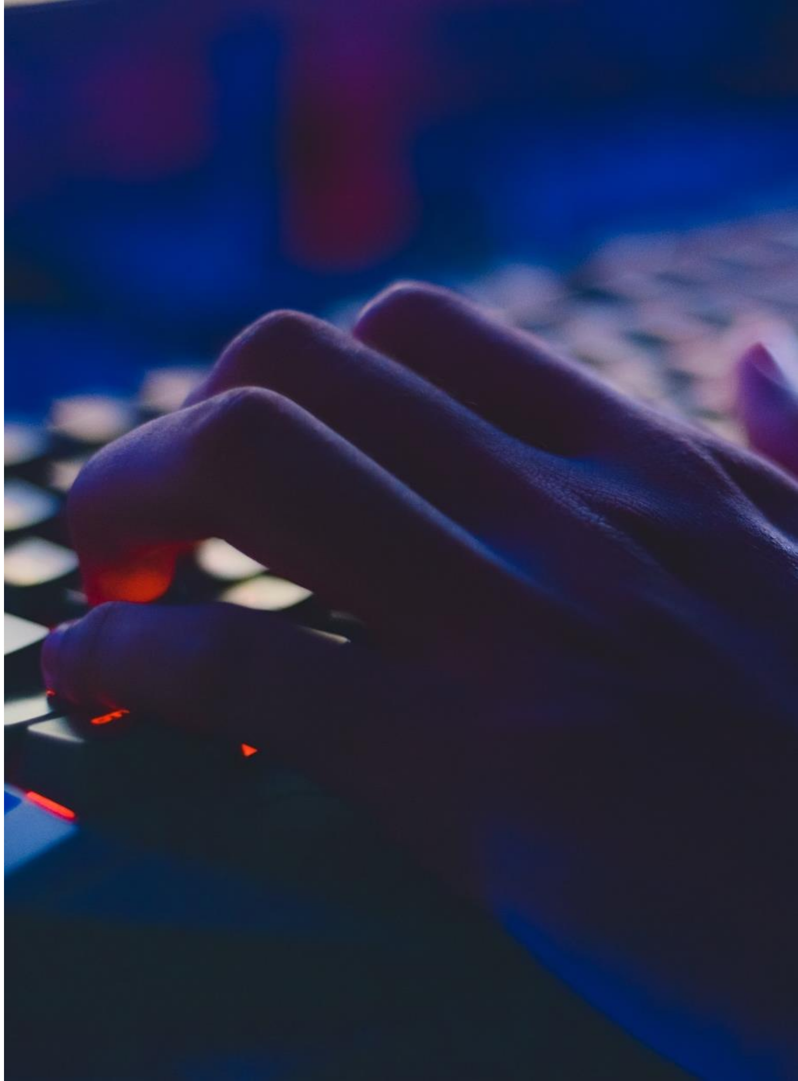
Higher risks are higher

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…

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…



Again: Higher risks are higher

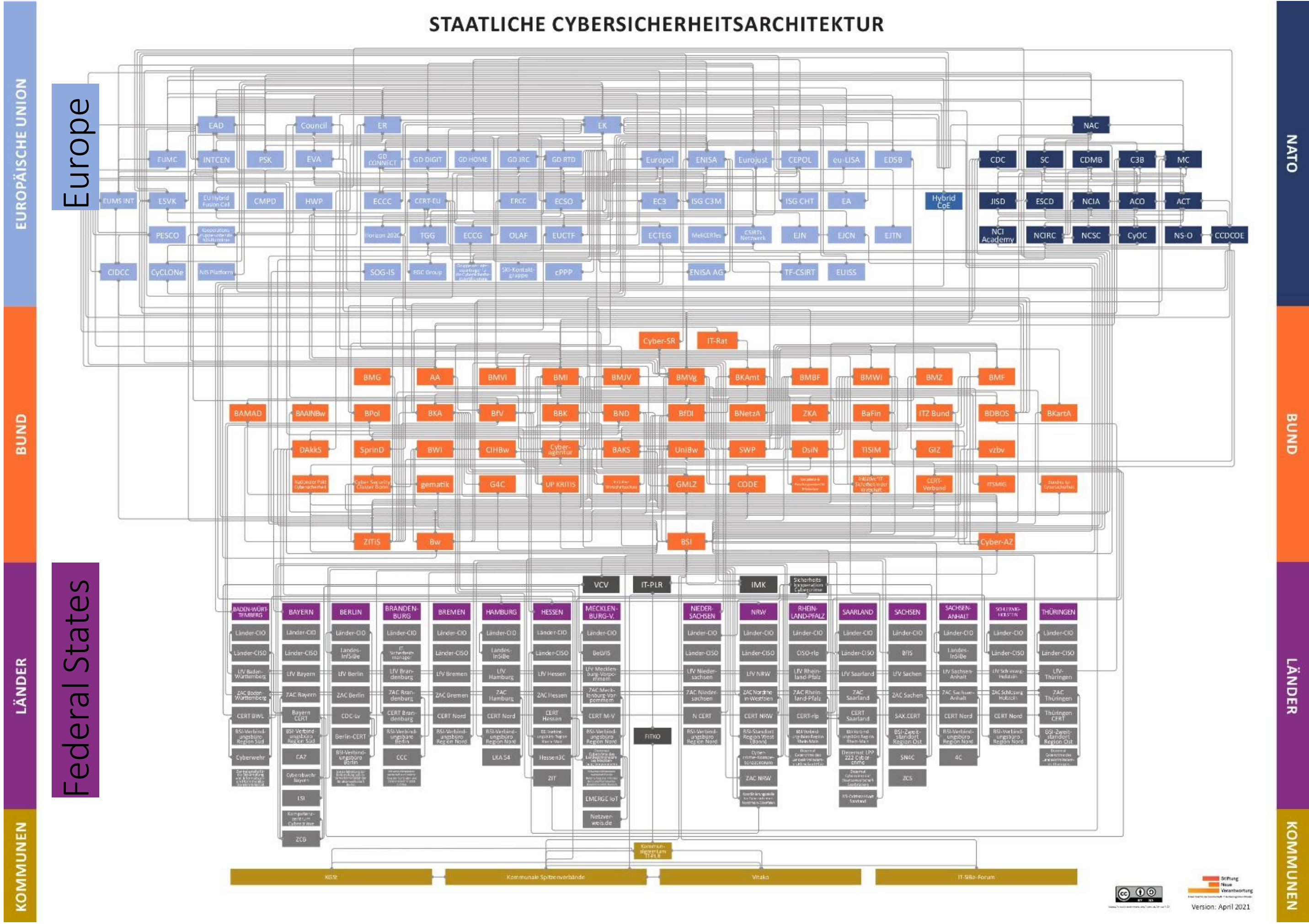
Threats become bigger

- cyber warfare
- Professionalized Cybercrime
- Organized Crime methods
- IT dependency
- 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



Europe

Germany

Federal States

Municipalities

IT-Security Law 2.0

Fear and sanctions

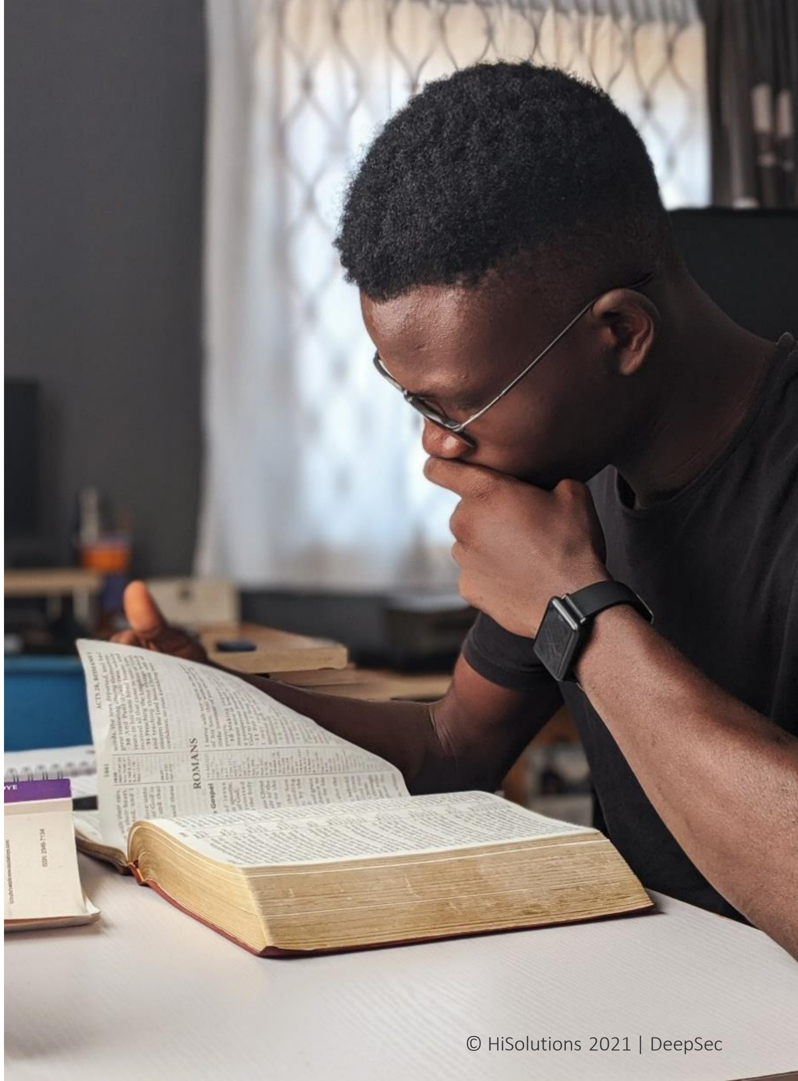
Draft: Federal Office for Information Security (BSI) should provide security vulnerabilities to security agencies and keep them secret for a “temporary time frame”

Done: „Lex Huawei“

Foreign Intelligence Service Law (BND Law)

Double standard

In parallel to the IT-SiG 2.0 the BND has received the legal right by law to hack into foreign Telco environments (aka KRITIS)



Cyber Security Strategie

Not a strategy at all

- “Security by encryption, security despite encryption”
- Hackback aka active cyber defence (Basic Law Amendment required)
- Digital souvereignity (via LI Methodology from ZITiS)
- Vulnerability Equities Process (VEP)

Solutions anyone?

Curse of competence for KRITIS

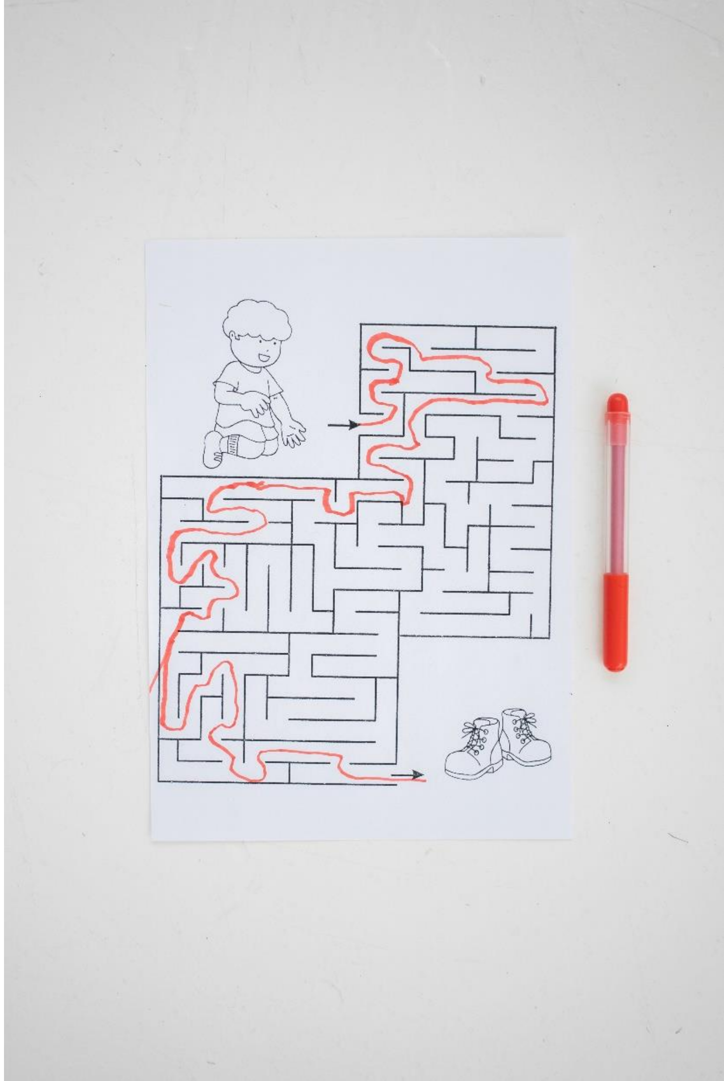
Cyberresilience and fallbacks

Do you all know how you would do the processes with **pen & paper**?

Happy happy joy joy

How to really enhance Cybersecurity

- Cyber resilience is key to success
- Defensive instead of offensive
- Positive error culture
- Organizational and communication culture
- Scientific and transparent evaluation of laws
- Use and incorporate feedback from InfoSec Community
- Use feedback channels and learn from them
- A good law requires some time



Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com