Cybersecurity technology day

CAN in Automation (CiA)

Manuel ‚HonkHase‘ Atug

Critical infrastructure security

Manuel ‚HonkHase‘ Atug

Manuel ‘HonkHase’ Atug

Head of Business Development at HiSolutions AG

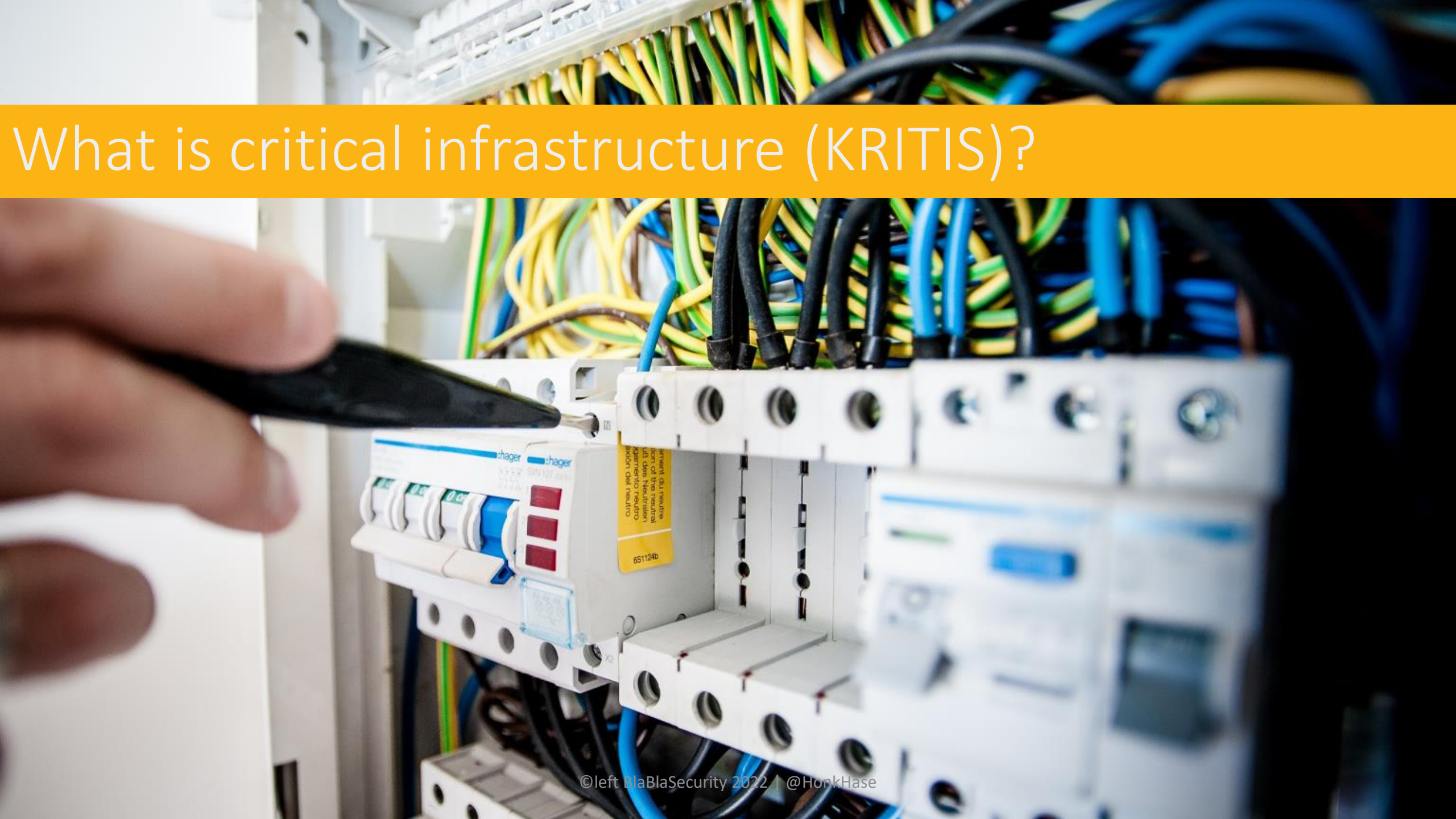
- Graduate computer scientist, Master of Science in Applied IT Security, Engineer
- > 23 Jahren in der Informationssicherheit tätig
- Topics: KRITIS, Hackback, Ethics, Hybrid Warfare, Cyberresilience, Civil Protection

- Founder of AG KRITIS: https://ag.kritis.info
- @HonkHase

AG KRITIS

I have #KRITIS in the final stage

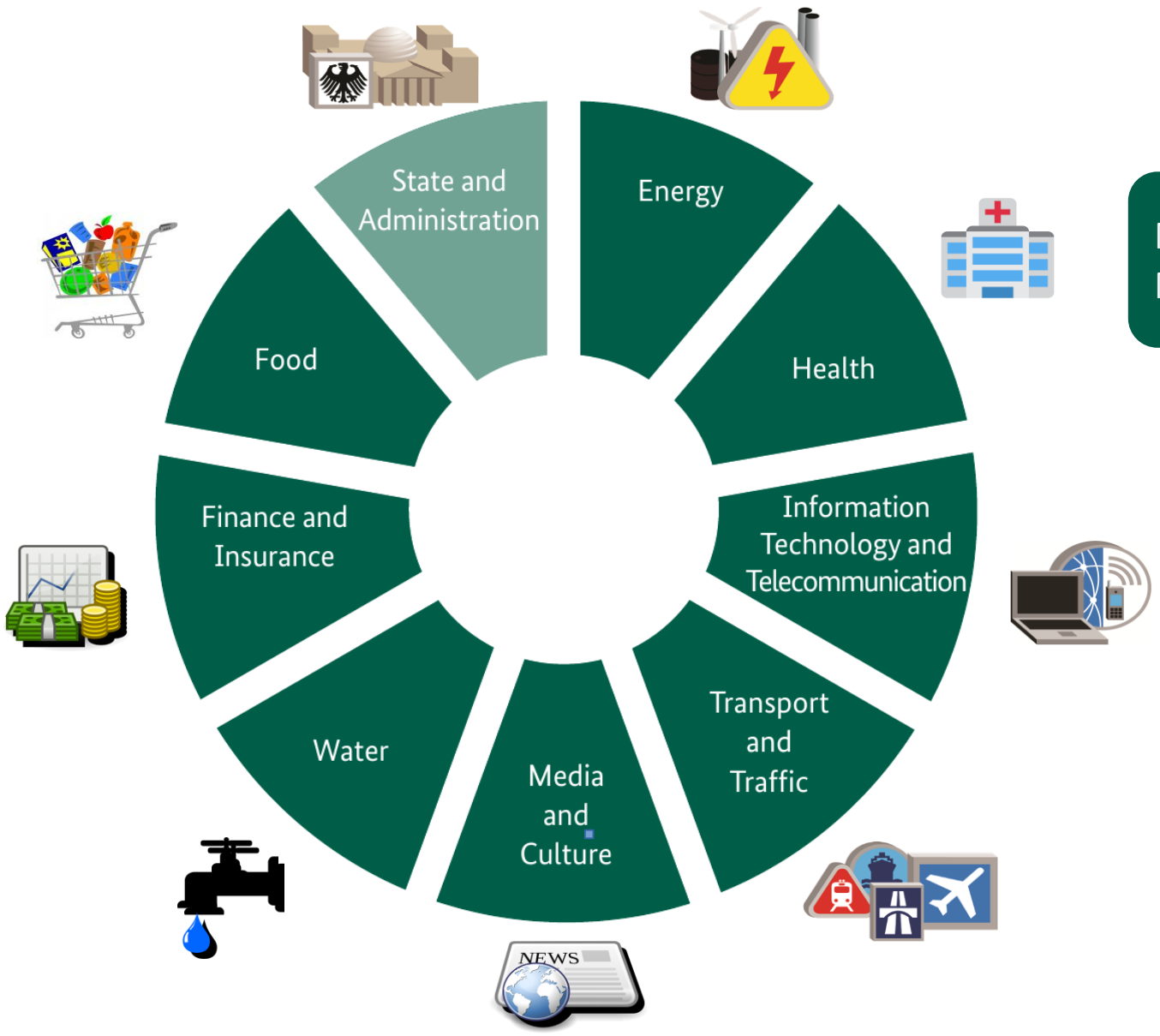
What is critical infrastructure (KRITIS)?



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

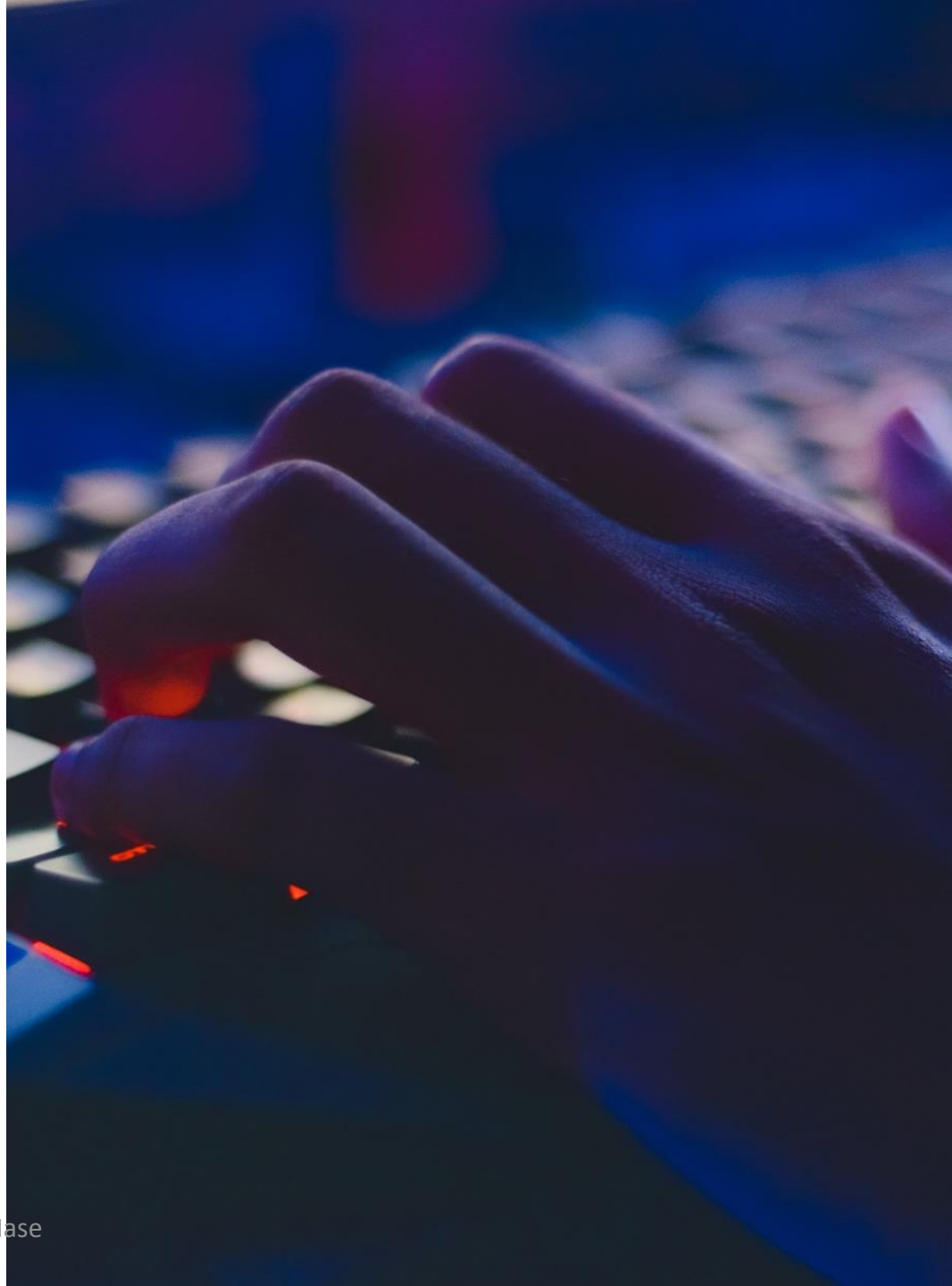
Higher risks are higher

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…

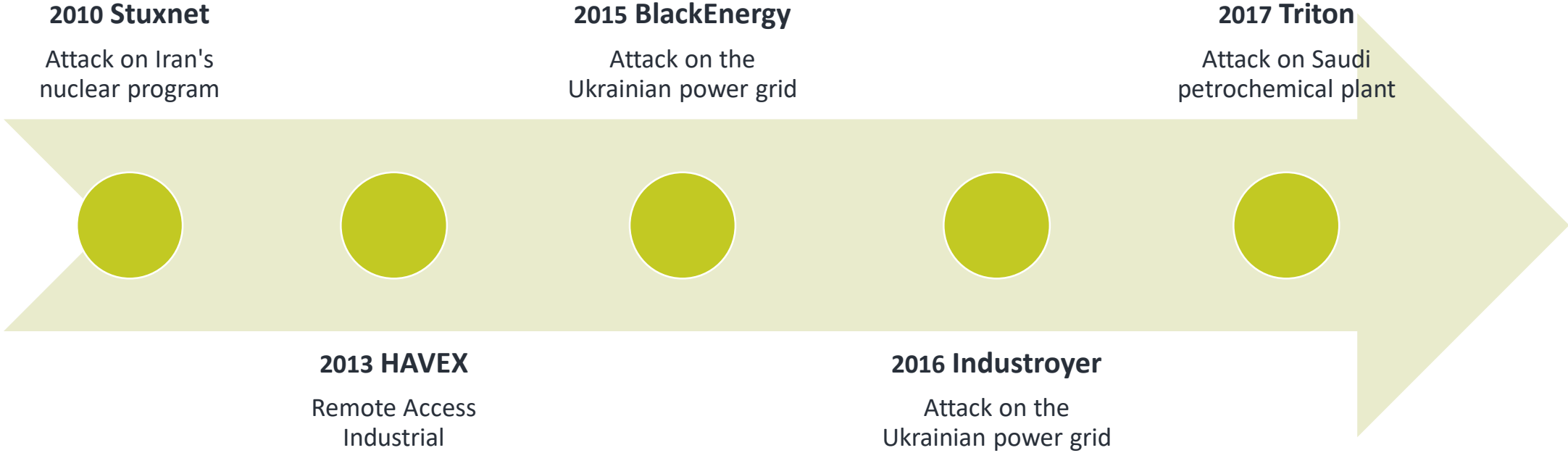
Ransomware

- 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



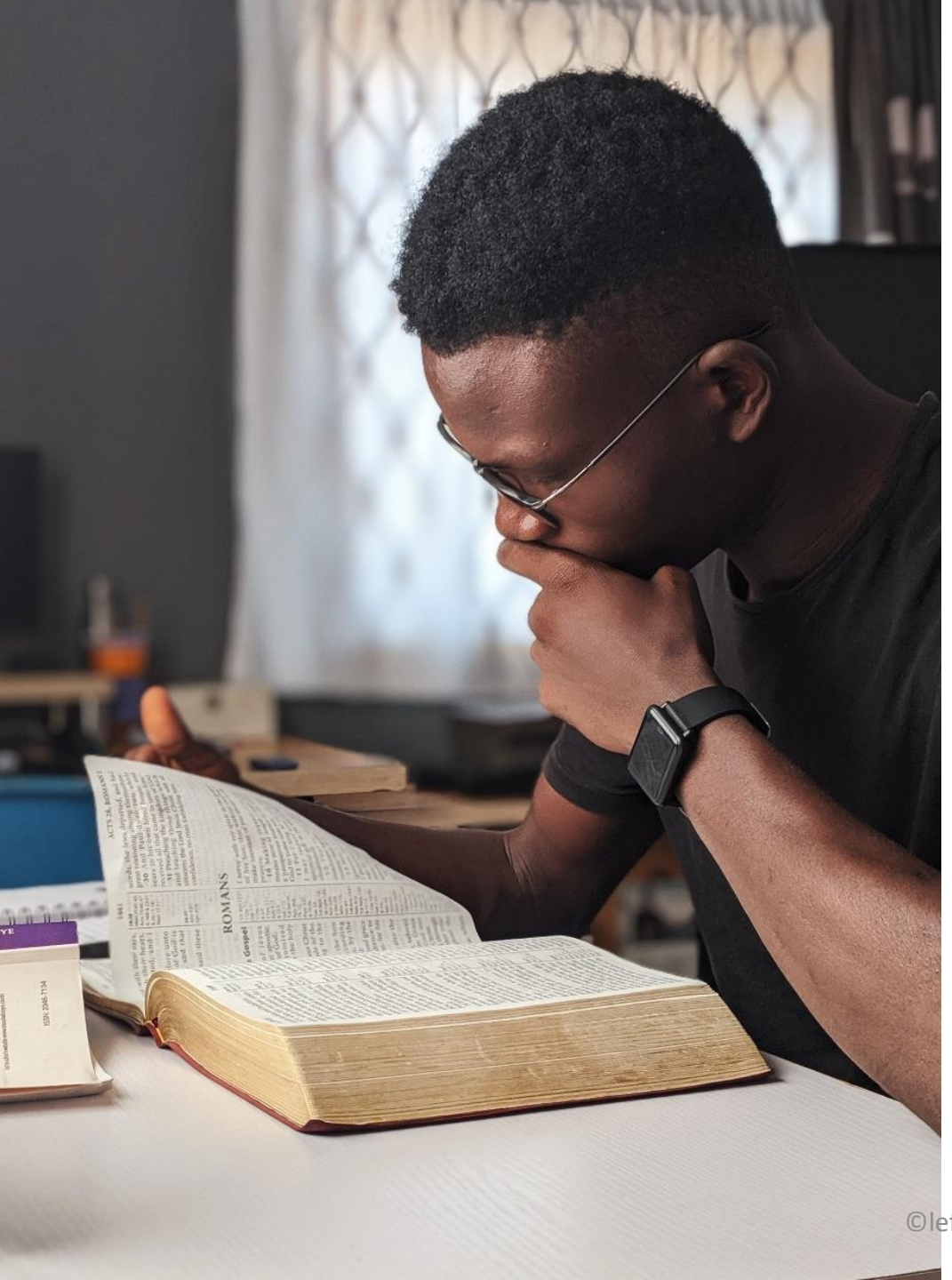
Again: Higher risks are higher

Threats become bigger

- 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>



Curse of competence

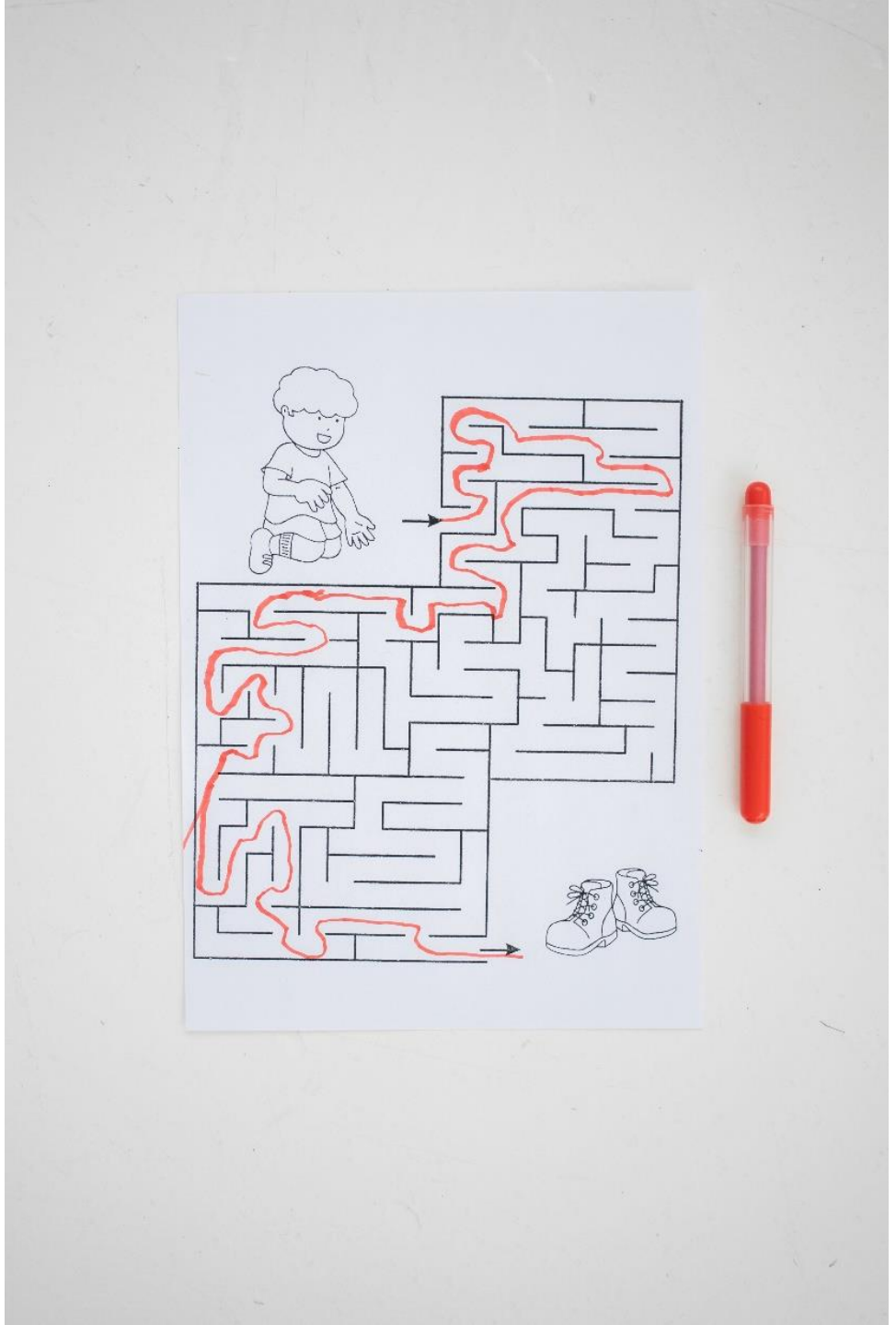
Resilience and fallbacks

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

Happy happy joy joy

How to enhance security

- Cyber resilience is key to success
- Defensive instead of offensive
- Positive error culture
- Report, discuss and exchange
- Use and incorporate feedback
- Use feedback channels and learn from them



All together? All together!

Always remember:

- IT Security is not a one man show
- They also only cook with hot water
- No magic silver bullet available
- Together you are strong
- Together you see more than individually
- Work hand in hand all together
- Know and use your ISMS and your BCM
- Did I already mention positive error culture?

And what do I do when all else fails?

Something with wood?

Coconut picker!

www.kokosnusspflücker.de **(german only)**