Critical infrastructure protection in energy sector – The challenges of cyber defence against hybrid warfare

János Ivanyos

ACER EWG Cybersecurity Task Force Co-convenor

MEKH Security Department

Meeting of ERRA Member Chairmen, Presidents and Commissioners
October 28, 2024 | Tirana, Albania

Hosted by:

Hybrid attacks on critical infrastructure 1

MEKH
Hungarian Energy and Public Utility Regulatory Authority

Use of cyber-attack as a tool in geopolitical conflicts

- Increased cyber activities targeting critical infrastructure, including energy and transportation sectors (Ukraine-Russia 2015-2024)

Risks associated with supply chain vulnerabilities

- Compromised SolarWinds' Orion software, affecting numerous organizations in various sectors including government and critical infrastructure (2020).

Hybrid attacks on critical infrastructure 2

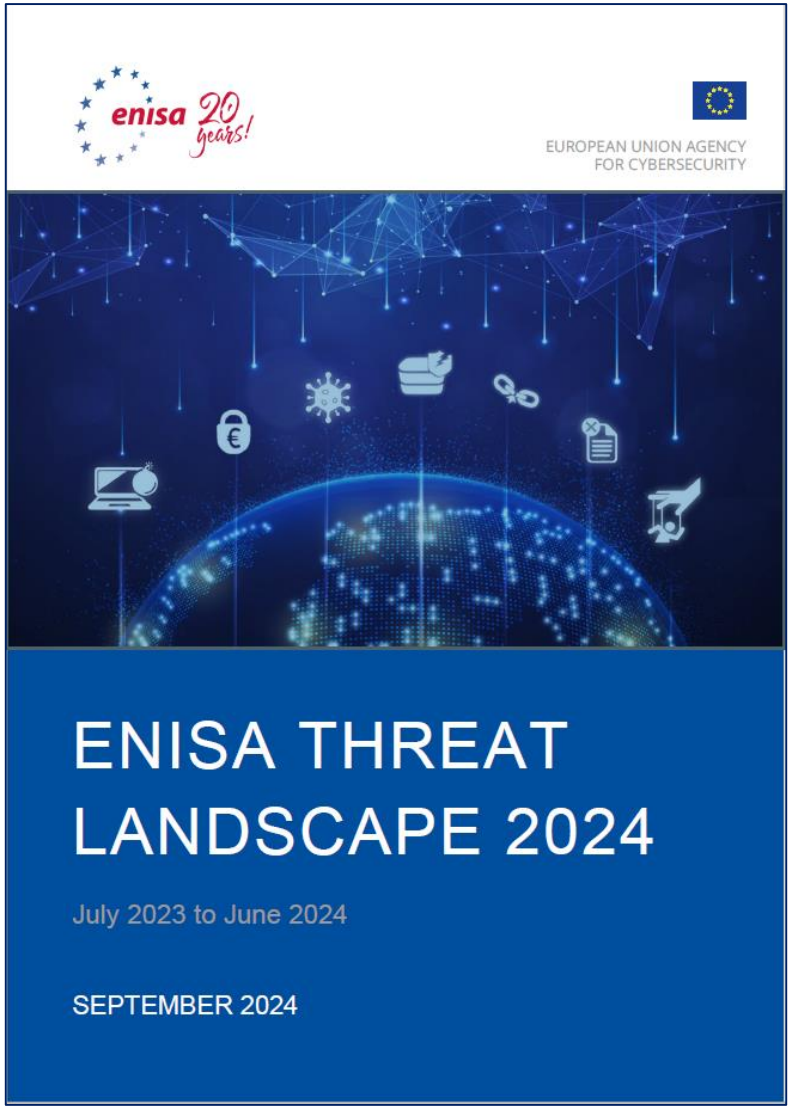
Large scale simultanious cyber attacks

- Targeted many companies at the same time, avoiding that impacted infrastructure could have shared information on the attack with peers.
- State-sponsored planning and resources.
- Coordinated attacks on Danish critical infrastructure (2023)

https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

Threat motivations

- **Financial gain:** any financially related action (carried out mostly by *cybercrime groups*);
- **Espionage:** gaining information on IP (intellectual property), sensitive data, classified data (mostly executed by *state-sponsored groups*);
- **Destruction:** any destructive action that could have irreversible consequences;
- **Ideological:** any action backed up with an ideology behind it (such as hacktivism).



Threat Actors

MEKH
Hungarian Energy and Public Utility Regulatory Authority

Categories:

- Cybercriminal 50%
- State-sponsored 40%
- Hacktivist 10%

Origin:

- China (17%)
- Russia (9%)
- Iran (5%)

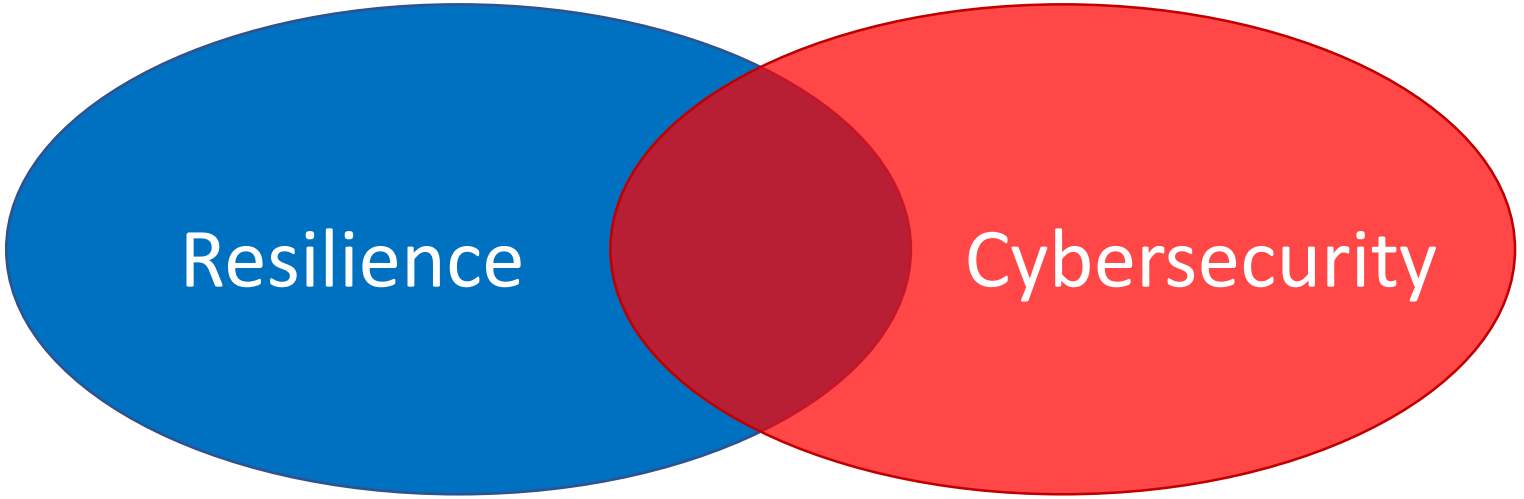
Targeted countries (T10):

- US
- Germany, India, Australia
- UK
- France, Italy, China, Japan, Canada

Targeted industries (T10):

- Government
- Financial services
- Technology, Telecommunication
- Media, Education, Healthcare, Energy
- Manufacturing, Retail

Challenges of hybrid defence 1
Risk Management



RISK

PREPAREDNESS & MITIGATION

- Similar risk impact on society, economy, military, environment, etc. -> same impact metrics
- Different occurance (vulnerability, threat, attack) types -> likelihood vs severity (metrics)

Challenges of hybrid defence 2
New accents

MEKH
Hungarian Energy and Public Utility Regulatory Authority

- Dependence from supply chain
- Simultaneous attacks (cross-border impact)
- Enhanced cybersecurity controls
- Real time detection and reaction
- Crisis management

- Controls of (ICT) products & services, supplier contracts
- Knowledge & information sharing
- Cybersecurity maturity development
- Exploiting artificial intelligence
- Planning & testing (exercises)

Why should energy regulators be involved in hybrid defence?

- In-depth sectoral (risk impact) knowledge (market, technology, participants, etc.)
- Relations between stakeholders (authorities, consumers, system operators, generators, traders, etc.)
- Sectoral level risk preparedness (or equivalent) functions (supervison & exercises)
- A type of independence from the government (trust issue)

ERRA Workshop hosted by MEKH, Budapest, February 20-21, 2025 – Day 1

MEKH
Hungarian Energy and Public Utility Regulatory Authority

- ERRA cybersecurity survey results
- Key definitions, threat landscape and previous cyber (hybrid) attacks in the energy sector
- IT/OT system related challenges from supply security perspective
- Cybersecurity related regulations and their consequences on Energy Regulatory Authorities in the EU
- Risk treatment methods of cyber attacks (Case Study)

ERRA Workshop hosted by MEKH, Budapest, February 20-21, 2025 – Day 2

- Crisis management, lessons learnt from EU wide cybersecurity exercise in energy sector
- Applying cybersecurity controls and relevant standards
- Security Operation Centers and Computer Security Incident Response Teams
- Information sharing between entities and authorities
- Using AI in cybersecurity knowledge sharing (Case Study)

MEKH
Hungarian Energy and Public Utility Regulatory Authority

ERRA
ENERGY REGULATORS REGIONAL ASSOCIATION

THANK YOU FOR YOUR ATTENTION!

János IVANYOS
ivanyosj@mekh.hu

https://erranet.org/