Case study Slovakia

The impact of digitalisation and cyber security on critical infrastructure: the civil society’s view

Matúš Mišík, PhD.
Civil Society Forum (Slovak Foreign Policy Association)
Prepared for 8th Workshop of Eastern Partnership Energy Regulatory Bodies, Minsk 21-22 May 2019
Digitalisation in the energy sector
Cyber security and critical energy infrastructure

- Case of Slovakia
  - EU member state
    - General framework comes from the EU
  - Energy policy/security an important issue
    - Especially after the 2009 gas crisis
    - Transit considered to be crucial for energy security
    - Critical energy infrastructure has a high priority
- Shows complexity of the issue
- Can provide
  - Lessons and good practices
  - Room for improvement
Framework for cyber security within the EU

- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
  - Article 5: Operators of essential services
    - (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
    - (b) the provision of that service depends on network and information systems; and
    - (c) an incident would have significant disruptive effects on the provision of that service.

- Energy infrastructure fits this definition
- Directive transposed to Slovak legal system
  - Act 69/2018 Coll. on Cyber Security
  - Much broader definition, includes mining and district heating
Hybrid threats

- **Cyber security part of hybrid threats**
  - Different issues, including "hybrid war", "fake news", etc.

- **Strategy for fight against hybrid threats**
  - Includes cyber threats, does not include energy
  - Defines the main hybrid threat in energy policy area to be dependency on energy imports from "a single external supplier"

- **Two types of threats**
  - Economic or political pressure
  - Sabotages against the critical infrastructure
What is the challenge?

• There is cyber security legislation
• However, it is separated from other hybrid threats
  o Defined in the Strategy for fight with hybrid threats
• Different authorities responsible for these issues
  o Limited cooperation

• How this problem manifests in energy policy?
  o Strategic energy policy documents do not mention hybrid issues
    • Energy policy, Energy security strategy, etc.
  o Focus on “traditional” energy security issues
    • Security of supply
  o This is also part of the discussion, but not the whole “story”
    • Cyber issues are not covered in energy policy discourse
    • Individual companies have cyber security strategies, however, common approach is missing
Why focus on cyber threats? I

- Focus on “traditional” energy security issues is problematic
- There are strategies and tools focused on these issues
  - There are also authorities that have been dealing with these issues
  - Only limited discussion between authorities
- Issues have been improved in this area
- Diversification
  - New interconnections: SK-HU, SK-PL, reverse flow with AT and CZ
  - Different situation compared to 2009 (the gas crisis)
Why focus on cyber threats? II

- No complex approach within energy policy
- Transit is considered to be important for Slovak energy security
  - Therefore projects like Eastring
- High share of electricity from nuclear
  - Even bigger share after finalization of Mochovce 3&4
- An important part of hybrid threats
  - Complex approach
    - Improved coordination, better cooperation among authorities
Recommenations

• **Increase focus on cyber threats within energy policy**
  o In strategic documents

• **Improve communication between individual agencies responsible for different hybrid threats**
  o Ministry of Interior, Ministry of Economy, Ministry of Foreign Affairs, National Security Authority

• **Put more focus on specificities of energy sectors**
  o The sector is crucially interconnected with the rest of the society with “hard security” consequences in case of cyber/hybrid attack on energy infrastructure

• **Include „smart technologies“ into the discussion**
  o Cyber attack countemeasures an important part of these technologies
Thank you for your attention

matusmisik@gmail.com

https://www.researchgate.net/profile/Matus_Misik