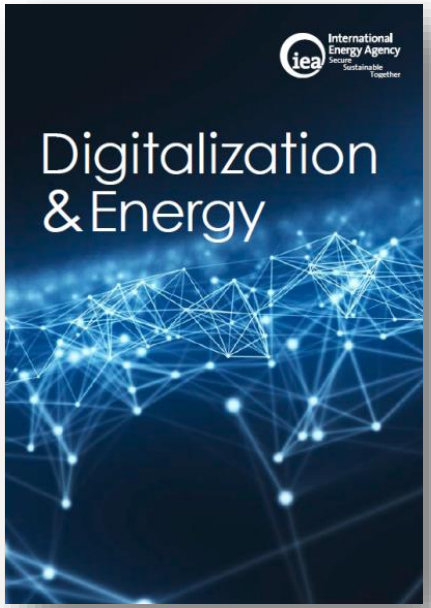
Energy and cyber security

"What cyber security means for the power generation industry?"

Jan Bartoš | Energy and cyber security policy analyst

ata insights **WEBINAR**

Digitalization & Energy – report by International Energy Agency

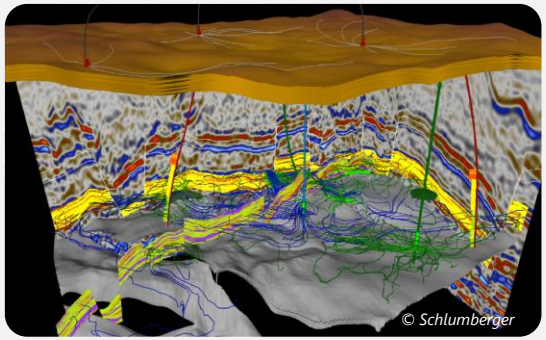


iea.org/digital

Provides good overview and introduction to the subject of digitalization of the energy sector:

1. **Introduction: A new era of digitalization in energy?**
2. **Energy demand: transport, buildings, and industries**
3. **Energy supply: oil and gas, coal, and power**
4. **System-wide impacts: from energy silos to digitally-interconnected systems**
5. **Energy use by digital technologies**
6. **Cross-cutting risks: cyber security, privacy, and economic disruption**
7. **Policy, including no-regrets recommendations**

Digitalization brings many opportunities!



Oil and gas

- Increased productivity, improved safety and environmental performance
- Could decrease production costs by 10-20%; recovery could be enhanced by 5%.

Coal

- Coal mining can expect to see improved processes and reduced costs as well as improved environmental performance

Power

- Power plants and electricity networks could see reduced O&M costs, extended life time, improved efficiencies and enhanced stability
- Savings of USD 80 billion per year

Energy companies have been adopting digital technologies for years, to increase productivity, reduce costs, improve safety and environmental performance

Source: IEA 2018, Digitalization and Energy

… but also added risk

- Smarter connection and integration of energy technologies
  - Many benefits, but also:
- Increased vulnerability of energy systems due to digitalization
  - Cyber attacks
  - Cyber incidents
  - Growing interconnectedness
  - Natural events (e.g. space weather)

- Cyber security problem for all sectors but energy is particular – underlies all; can't be simply shut down
- Many examples from recent history show increase of incidents:
  - Targeted (Shamoon, Stuxnet, Ukraine, **Trisis**) and generic (global ransomware outbreaks - Wannacry)
- So far damage small in scale compared to other disruptions (geopolitical, natural)
  - Governments / companies need all-risk, cross-sectoral approach
- But attacks are becoming cheaper, need less sophistication, attack surface is larger

Trends to watch

- Growth of Internet of Things (IoT) / Industrial Internet of Things (IIoT) / IoE (Energy)
  - Diversification and decentralization of energy technologies
  - Millions of small-scale “prosumers,” billions of devices
- Geographic diversity of Internet (and companies) -> attack in one location can instantly spread (example WannaCry, NotPetya -> Maersk)
- Changing technologies also in centralized systems:
  - Past: reliance on proprietary, specific technologies; hacking requires specific knowledge
    - Therefore “security by obscurity”
  - Today shift to connectivity, automation, cloud computing, “security as a service”
    - More sophisticated open-protocol standards, but loss of obscurity
- Low probability, high risk scenarios of shutting down entire systems for days/weeks
- Increase of small-scale “nuisance” attacks from botnets

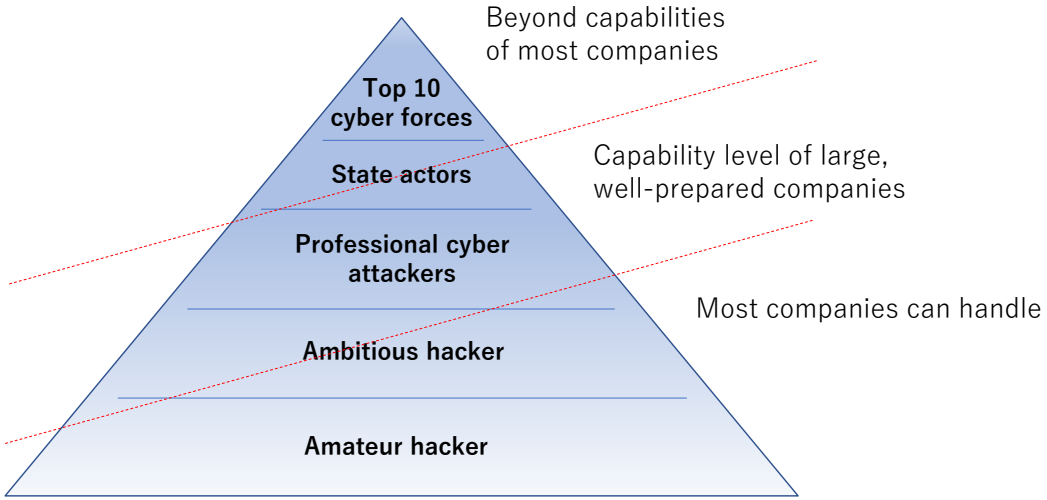
Building (digital) resilience

- **Key precondition: all actors aware of risks!**
  - Recent incidents repeatedly show unpreparedness and lack of basic principles (updating, patching)
  - Many energy companies still don't acknowledge cyber as major risk
- Cyber hygiene – awareness building, secure configuration, updates, trainings…
- Building resilience – ability to adapt, withstand shocks, recover quickly to basic service, preserve **continuity of critical infrastructure**
  - "Ecosystem" approach; no risk can be 100% prevented
- Mainstreaming cybersecurity and resilience into energy research, development, deployment
- Building consensus on definitions for concepts and technical specifications (standards)
- International efforts can help raise awareness and share best practices

Preparedness – sharing responsibility

Limiting impact (resilience) is particularly important for **critical infrastructure**: the physical and institutional assets that are essential for an economy to function, such as large-scale energy systems.

- Mexico: identified 3 000 “strategic installations”, half of them owned by the national oil company PEMEX and another 13% by the Federal Electricity Commission.
- Germany: any infrastructure on which more than 500 000 people (1/160th of population) depend is considered critical. This includes all gas power plants and electricity transmission grids.



Key message: The handling of some attacks falls within the capability of companies themselves, while larger-scale attacks by sophisticated actors may require more active government responses.

Best practices and policies

- In many countries cyber is already high on agenda and specifically deal with energy
  - Specialized institutions to provide real-time analysis and threat information
  - Catalogues of minimum IT standards for energy sector
  - Supervision of critical infrastructure operators
  - Some however developed cyber strategies without mentioning energy
  - EU: NIS Directive (Network and Information Systems)
- Large-scale and small scale exercises take place
  - E.g. North America, EU, Nordic countries…

No-regrets policy recommendations

1. Build digital expertise within their staff.
2. Ensure appropriate access to timely, robust, and verifiable data.
3. Build flexibility into policies to accommodate new technologies and developments.
4. Experiment, including through “learning by doing” pilot projects.
5. Participate in broader inter-agency discussions on digitalization.
6. Focus on the broader, overall system benefits.
7. Monitor the energy impacts of digitalization on overall energy demand.
8. Incorporate digital resilience by design into research, development and product manufacturing.
9. Provide a level playing field to allow a variety of companies to compete and serve consumers better.
10. Learn from others, including both positive case studies as well as more cautionary tales.

Key messages

- Raising awareness is crucial to defend against cyber risks
- Governments, companies and other stakeholders need to work together proactively to manage the increasing complexity of threats
- Digital resilience needs to be mainstreamed into policy and market frameworks, research

Feel free to contact me!

Jan Bartoš | **energy / cyber security policy analyst**

h_bartos@centrum.cz

linkedin.com/in/jan-bartoš-69232a50

@JanBartos1981