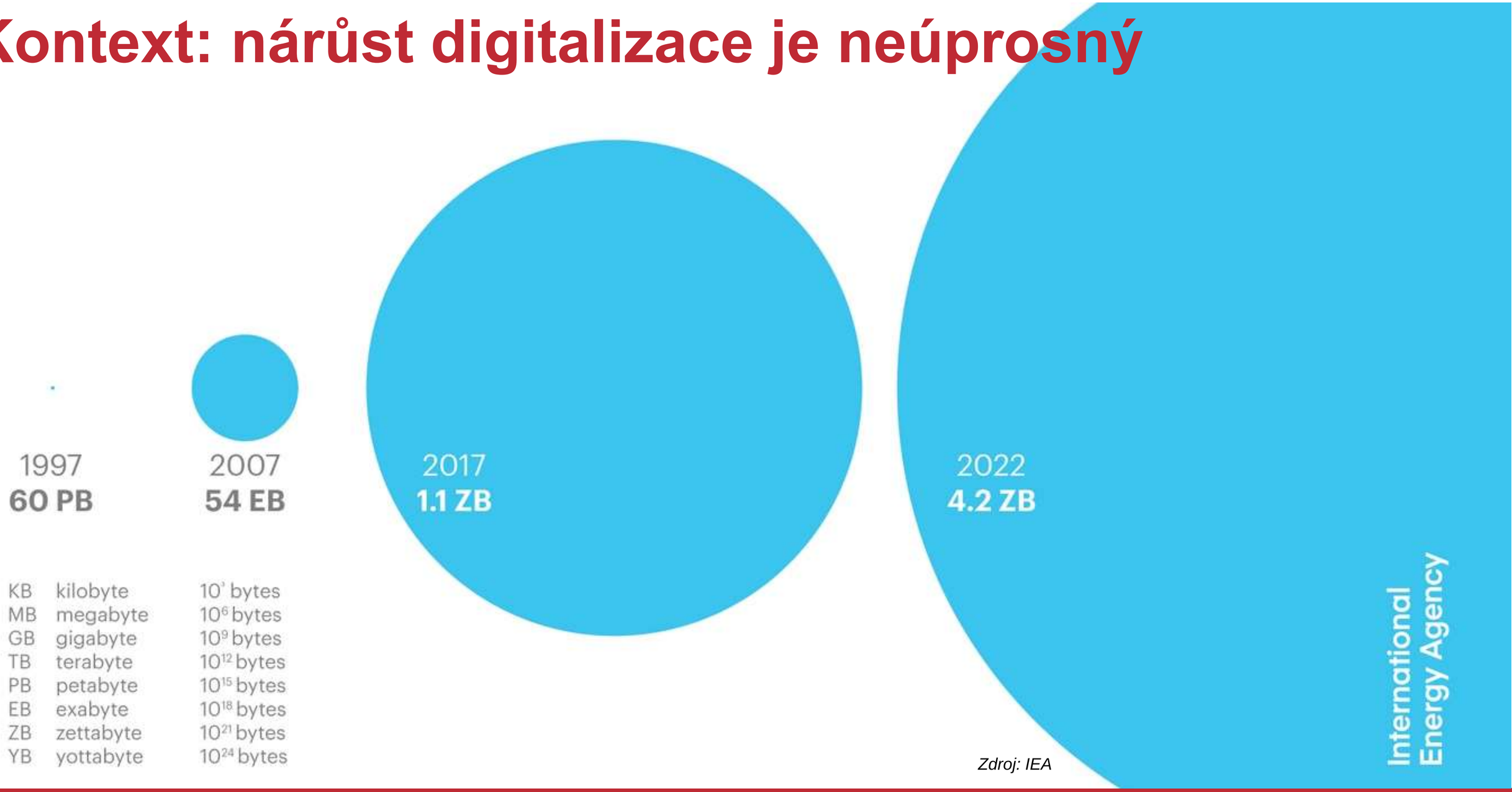
Digitalizace energetiky: příležitosti a rizika (v mezinárodním kontextu a z pohledu TSO)

Trendy české a evropské energetiky, 10. 11. 2020

Jan Bartoš, senior specialista odboru Digitalizace

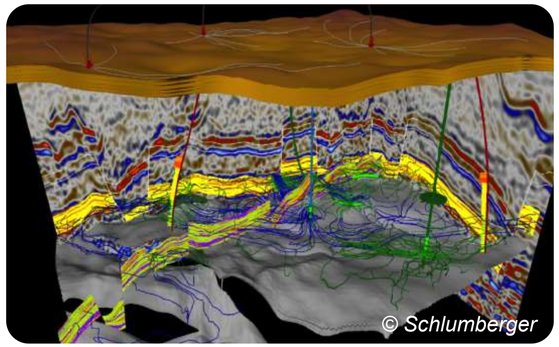
Kontext: nárůst digitalizace je neúprosný



Zdroj: IEA

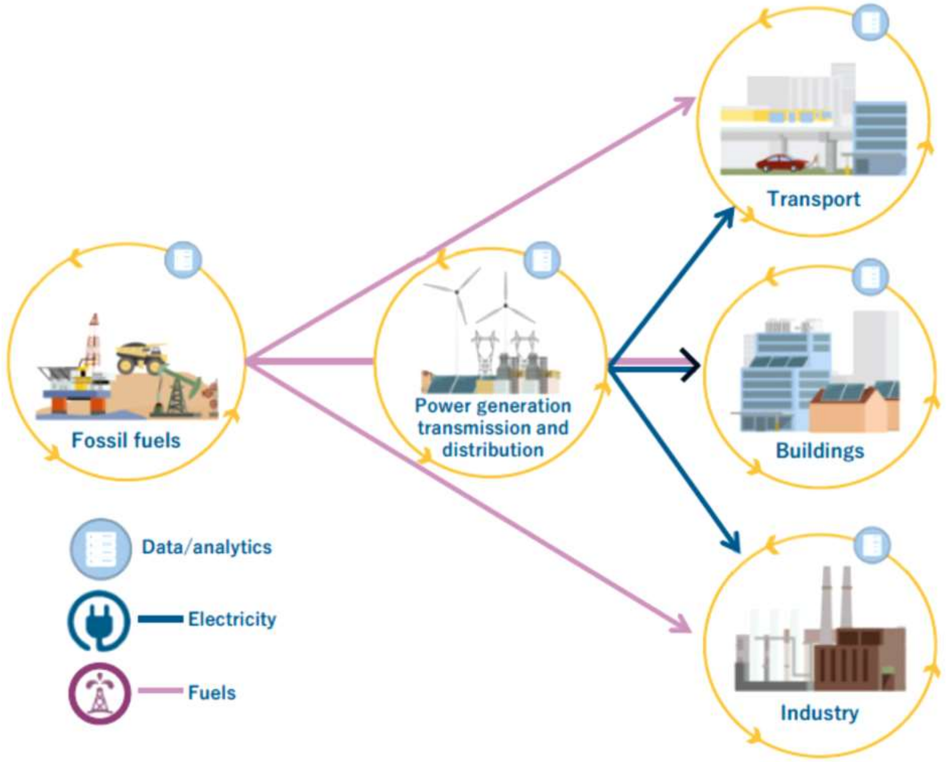
Energetika a digitalizace

- Digitalizace není v energetice nic nového
  - Produktivita, bezpečnost, snížení nákladů, snížení dopadů na ŽP
  - Týká se všech sektorů – „staré“ i „nové“
  - Největší revoluce v elektřině
    - Řešení pro variabilní OZE
    - Umožnění nových tržních mechanismů v souvislosti s decentralizací



Digitalizace z pohledu PPS (TSO)

Energetický sektor prochází zásadní proměnou



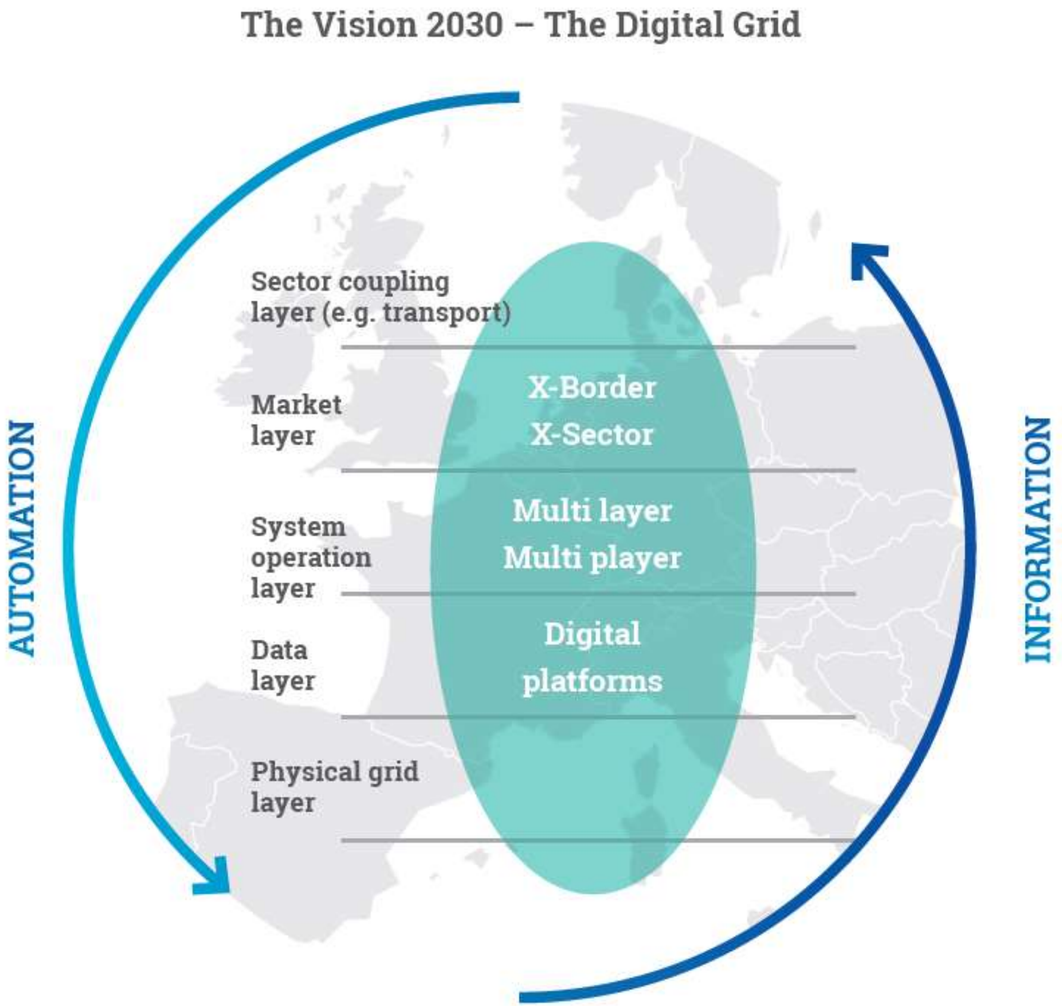
Dekarbonizace

Decentralizace

Digitalizace

Zdroj: IEA, upraveno

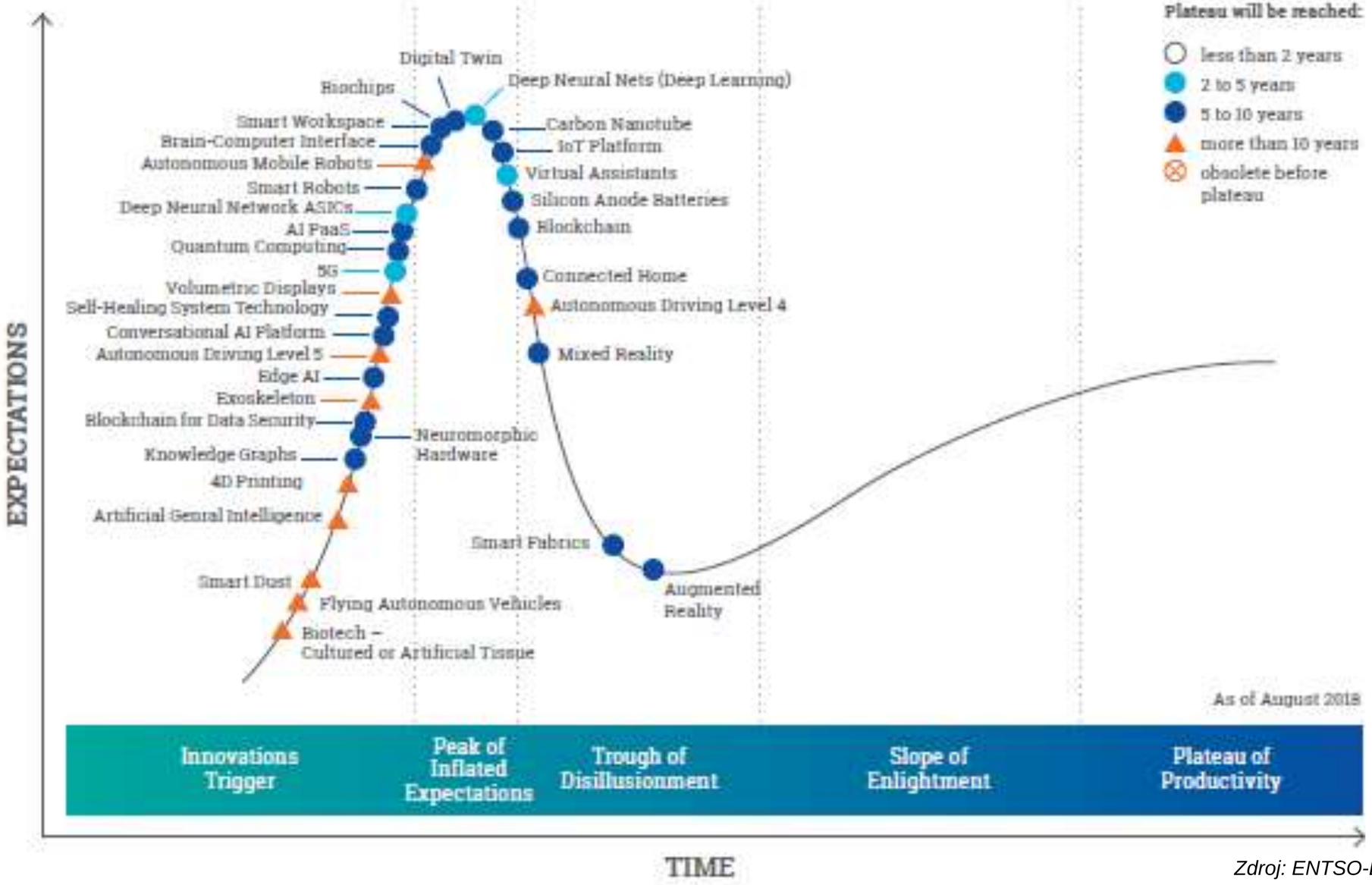
Spolu s tím se výrazně promění i role TSO



- Aktivní role ve směřování trhu
- Inter-operabilita, TSO–DSO
- Digitalizace hraje roli:
  - Fyzická síť (infrastruktura)
  - Řízení sítě
  - Nové podpůrné služby
  - Data
  - Propojování sektorů
  - Přeshraniční spolupráce
  - Standardizace

Zdroj: ENTSO-E

„Hype“ křivka



Zdroj: ENTSO-E / Gartner

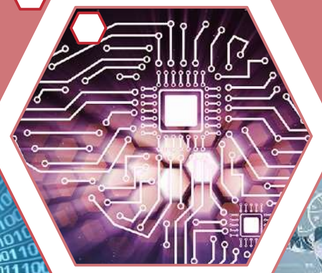
DigitalTwin – Digitální dvojče

Blockchain (Flexi a Agregace)

BIG DATA- Datové Modely

AI a Machine learning

UAV, Analýza obrazu



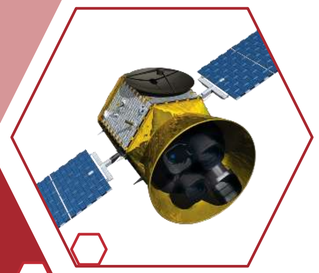
WAMS

Datová analytika

VR a AR

Robotizace a Automatizace

Kybernetická bezpečnost



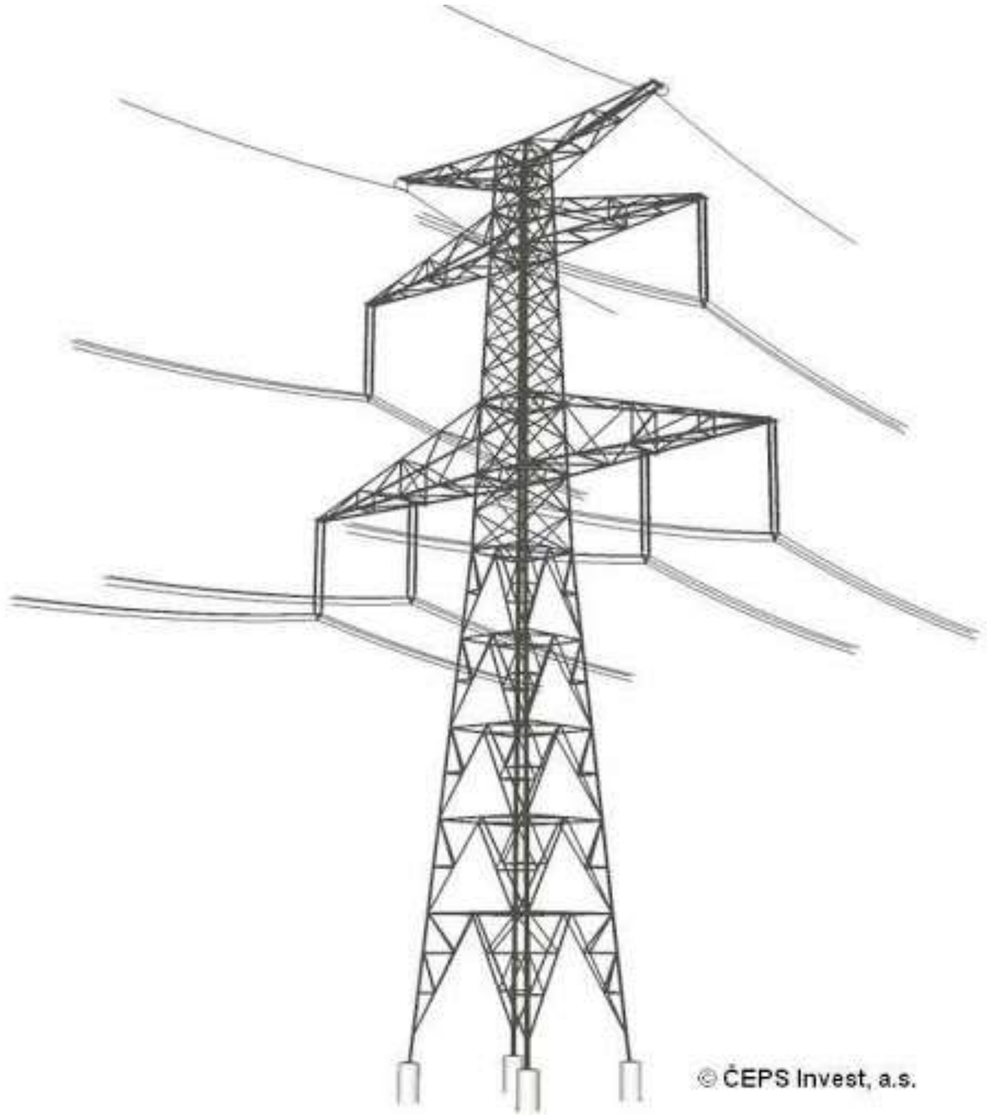
5G

Flexibilita a Crowd Balancing Prediktivní údržba

Jaké trendy sledovat?

Příklady z praxe

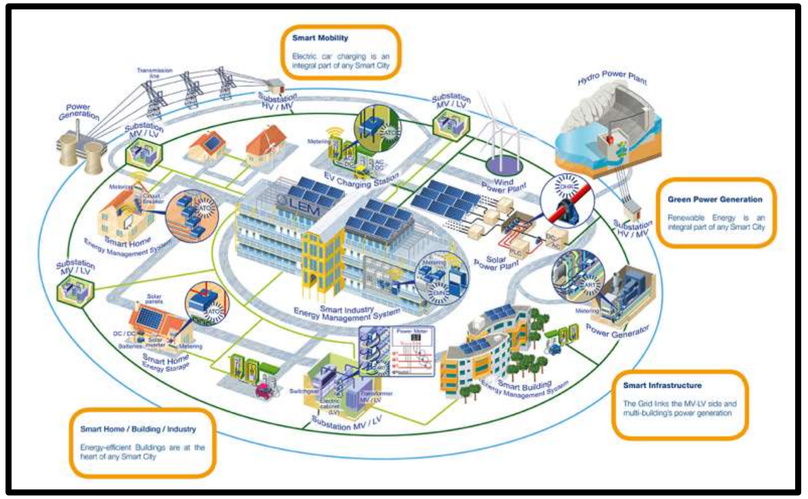
- Paperless
- BIM (Digital Twin)
- Blockchain – Crowd Balancing
- AI – predikce PS
- Open Source nástroje modelování PS
- WAMS (next-gen SCADA)
- Drony, VR
- 5G, Datová analytika, DataHub atd.

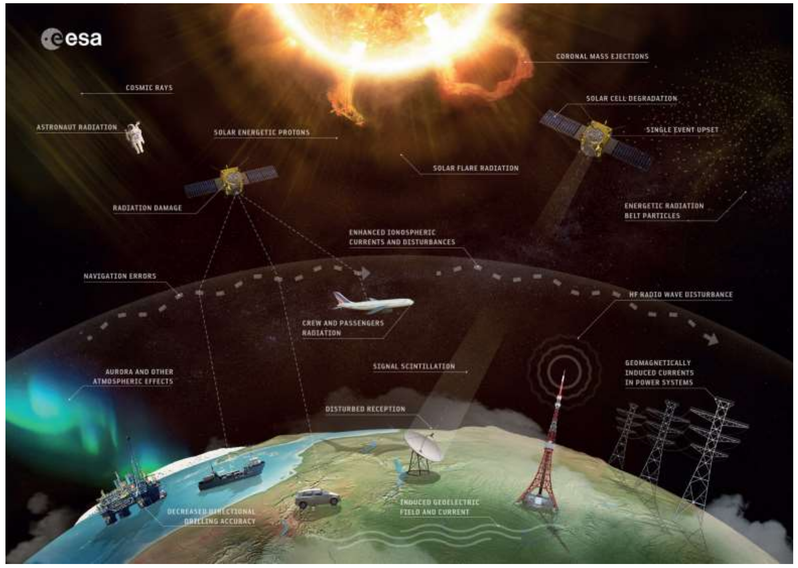


Rizika spojená s digitalizací

Digitalizace – zvyšuje riziko?

- Riziko **pro všechny sektory**
  - Energetika je specifická – **závislost ostatních sektorů**
  - Společnost očekává nepřetržitou dodávku energie
- Pokračující propojení, integrace na globální úrovni
  - **Kybernetický útok**
  - **Technické incidenty**
  - **Přírodní jevy** (geomagnetická bouře)
- Cílené útoky X vedlejší škody
  - Stuxnet, Trisis, Ukrajina X ransomware (Wannacry)
- Digitální riziko musí být nahlíženo spolu s dalšími (all-risk)
- Žádné riziko nelze eliminovat 100%

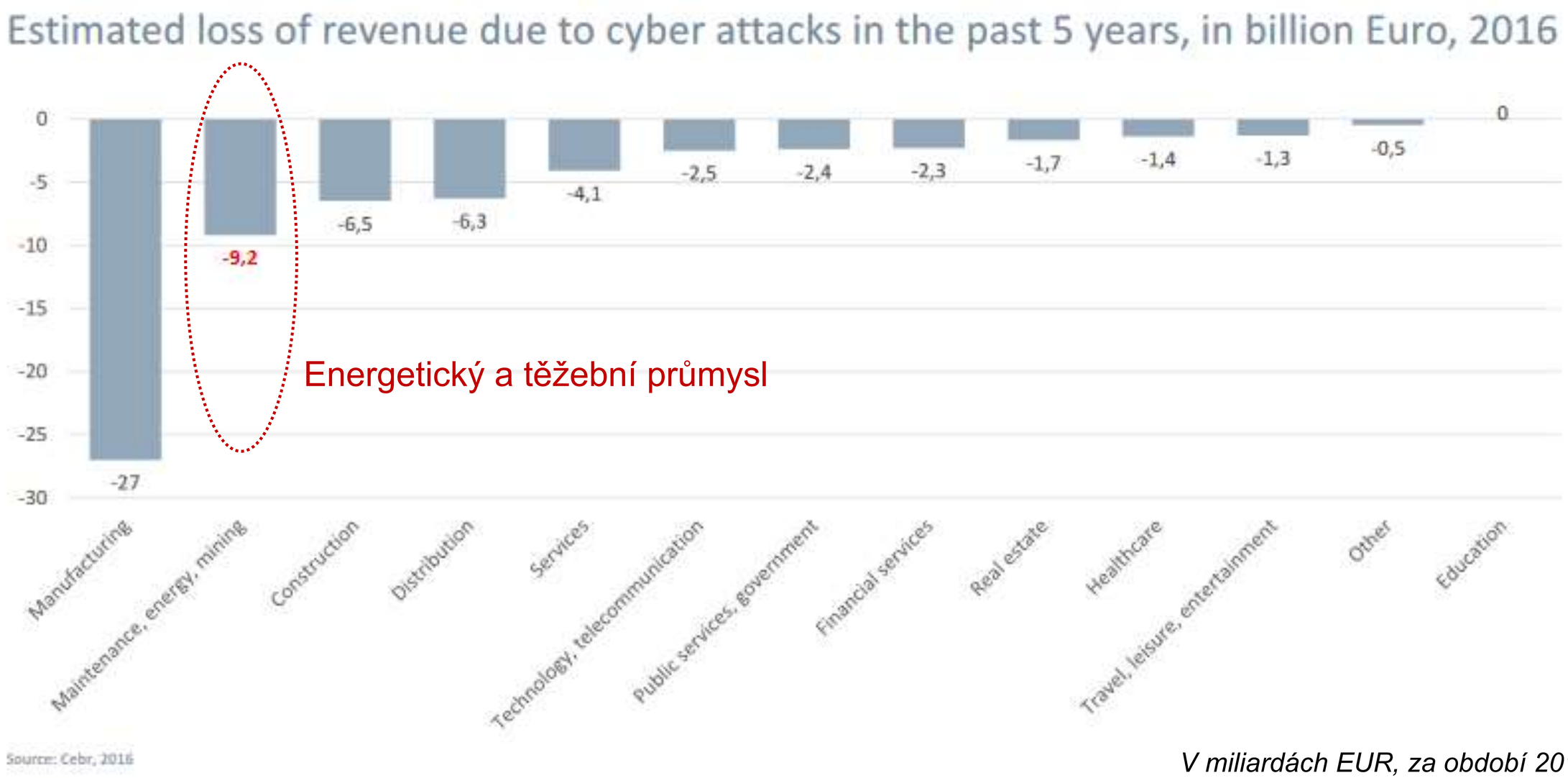




Čemu věnovat pozornost?

- Internet of Things
  - Diverzifikace, decentralizace
  - Miliony „*prosumers*“, miliardy připojených zařízení
- Globální charakter internetu a ekonomiky – útok v jednom místě se může okamžitě rozšířit
  - Příklad Maersk – NotPetya, Wannacry
- Výměna technologií i v centralizovaných velkých systémech
  - Rozsáhlé dodavatelské řetězce, řešení třetích stran
- Scénáře s nízkou pravděpodobností, ale vysokým rizikem dlouhodobého rozsáhlého výpadku (dny–týdny)
- Nárůst počtu drobných, otravných útoků od „botnetů“

Odhadovaný ušlý zisk v důsledku cyber útoků



Energetický a těžební průmysl

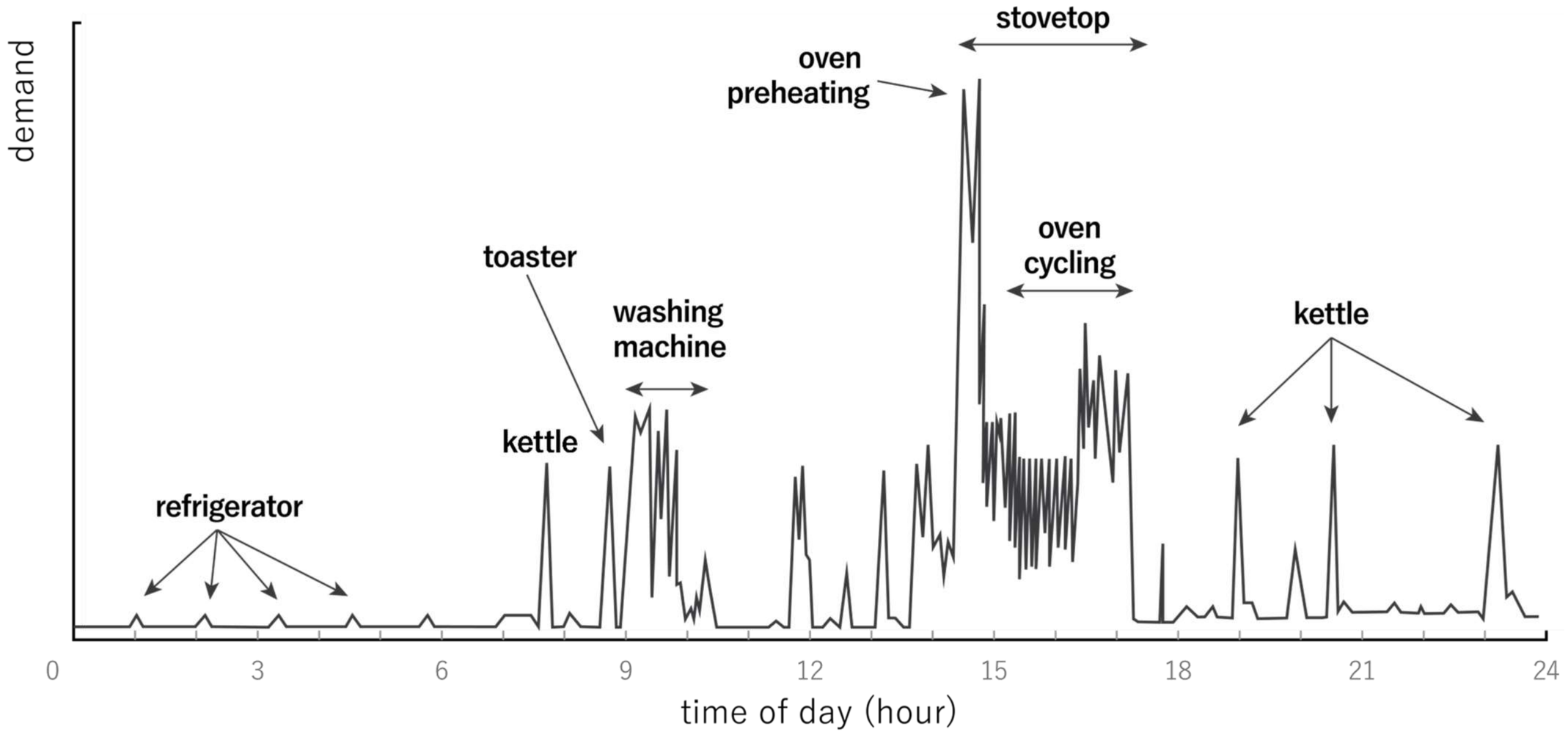
V miliardách EUR, za období 2011–2016

Důsledky podcenění připravenosti:

- Reputační
- Finanční
- Technické
- Operační
- V extrémních případech: ztráta zdraví / životů

- „Velké“ vs „malé“ firmy – „nás se to netýká?“

Data – poklad i riziko



Zdroj: *Newborough and Augood (1999), "Demand-side management opportunities for the UK domestic sector" (reproduced courtesy of the Institution of Engineering and Technology).*

Děkuji za pozornost

Jan Bartoš, senior specialista odboru Digitalizace

bartos@ceps.cz

ČEPS, a.s., Elektrárenská 774/2, Praha 10, www.ceps.cz