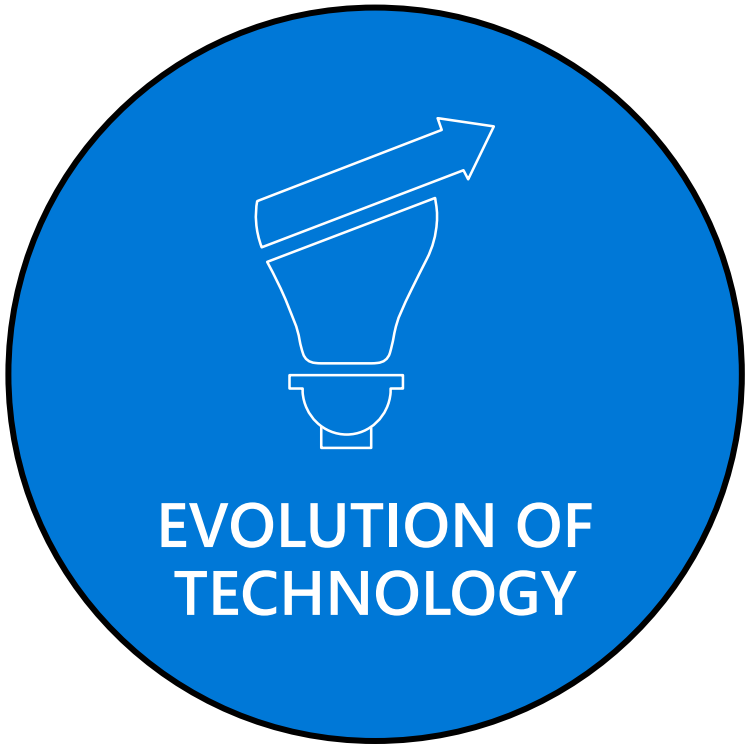
Microsoft

Investing in cyber resilience as critical infrastructure operators:

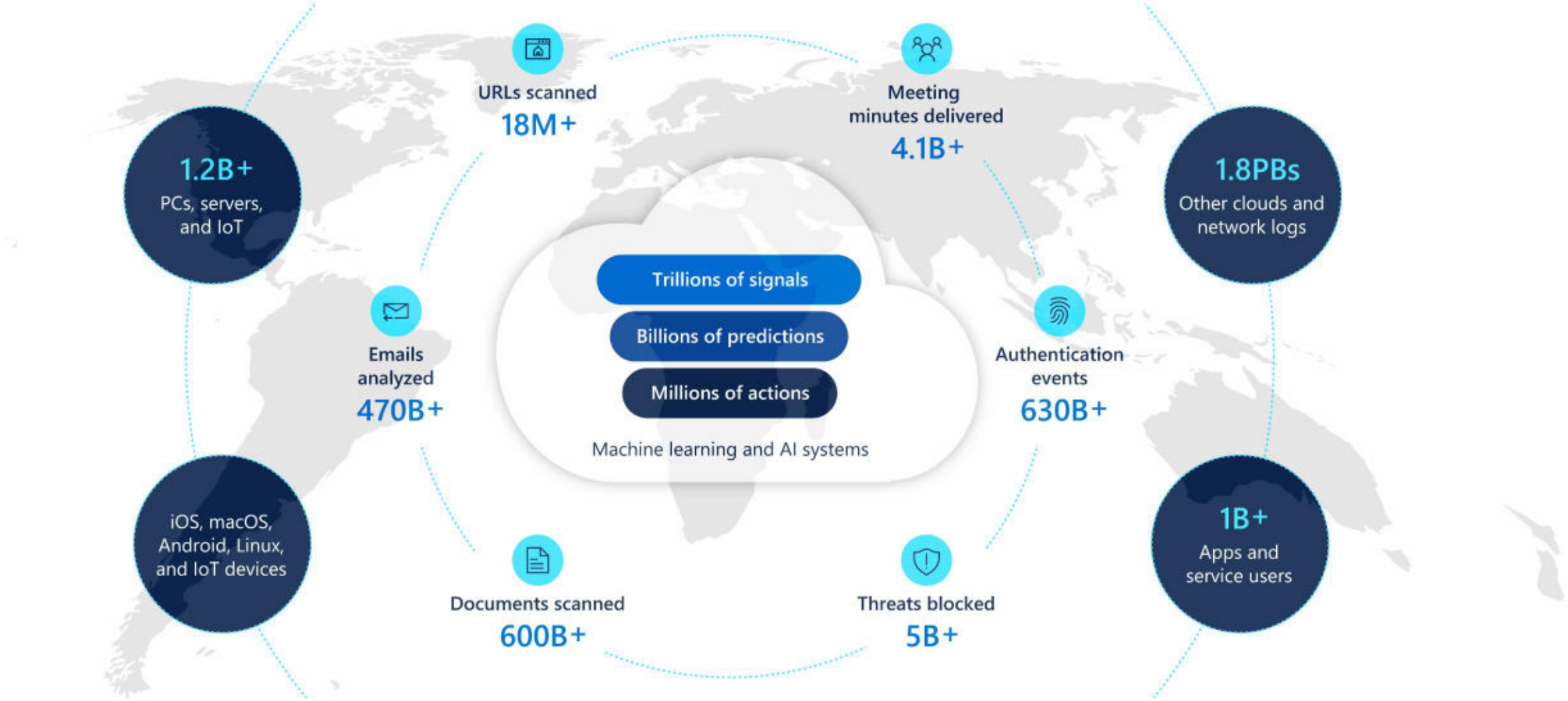
Regulation or cooperation?

New paradigm: From physical to digital



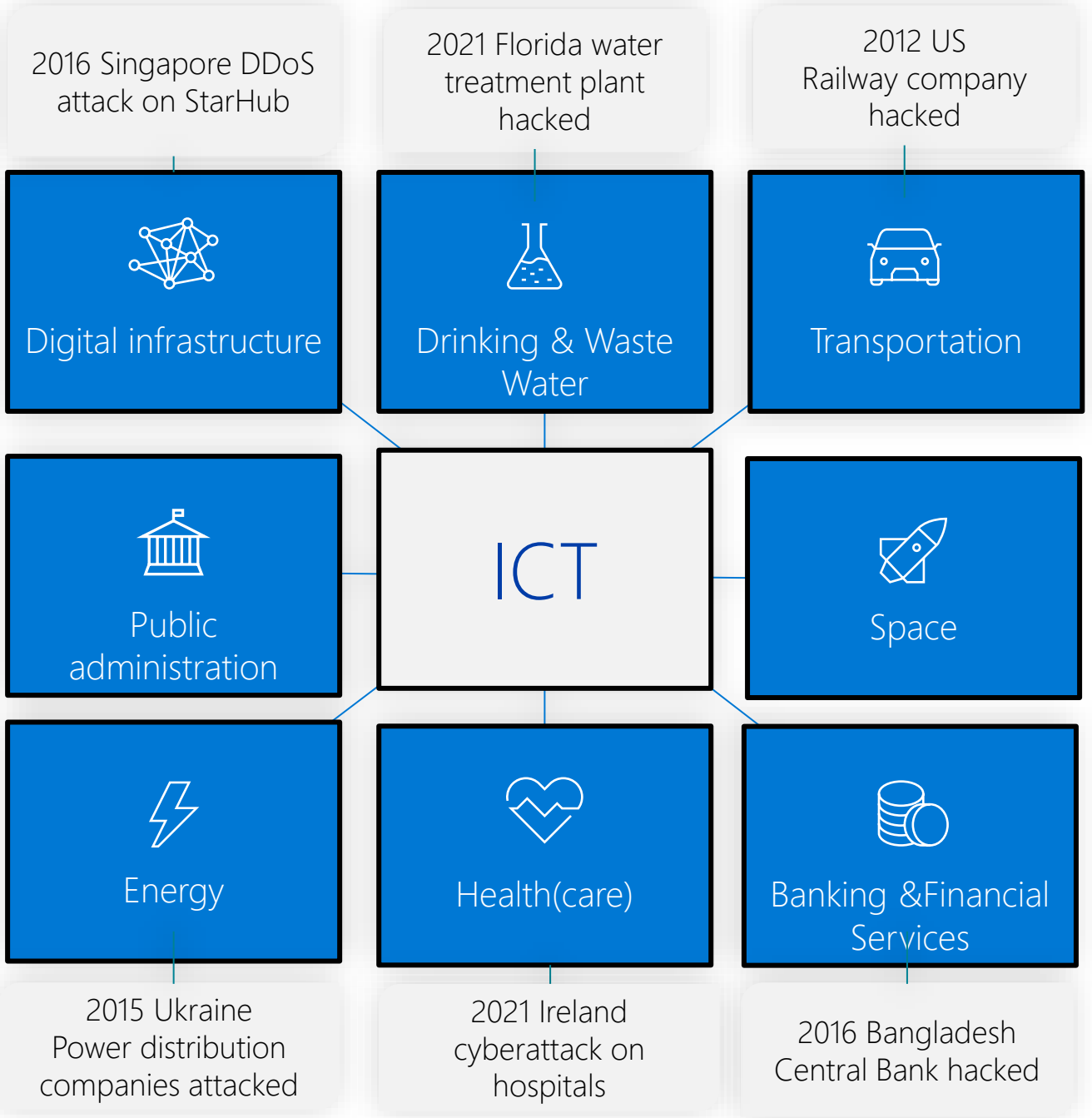
Trillions of security signals

Monthly volume and diversity of signals used by Microsoft security operations



Protecting critical infrastructure is increasingly important

Without appropriate safeguards, the proliferation of connected devices and big data will make critical infrastructure more vulnerable to a serious cyberattack.



Protecting critical infrastructure is a continuum

Critical infrastructure protection (CIP) is not an end state, but a continuous process of managing risk to improve security and resiliency.

- **Establishing trustworthy policies and plans** for protecting critical infrastructure in today's dynamic environment.
- **Managing risk**: Fostering capabilities for preventing, detecting, responding to, and recovering from risks to promote operational resiliency.
- **Promoting innovation and investments** by learning from policy and operations that can guide the allocation of resources for practices, programs, education, and research related to CIP.

How to respond anno 2021?

EU Cybersecurity legislation?

NIS2
Energy providers = Essential Entities

- Electricity (+ extention of scope)
- District heating and cooling
- Oil (+ extention of scope)
- Gas
- Hydrogen

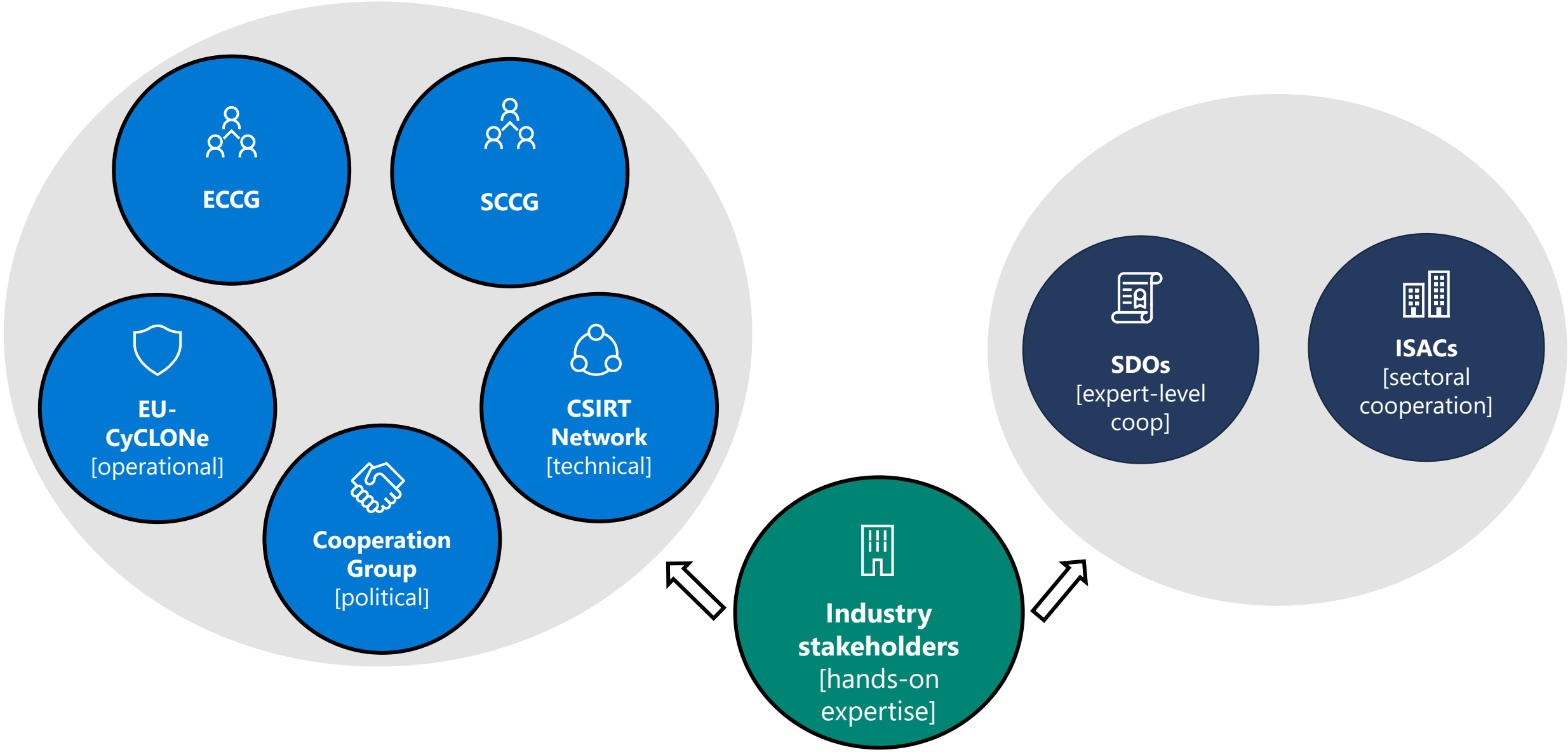
CER Directive

Cybersecurity Act – certification

Sector-specific legislation

- ACER consultation on Network Code on Cybersecurity
- DORA

Cybersecurity cooperation frameworks?



Future challenges:

Cybersecurity is global

Avoid fragmentation

Identify efficient solutions

Engage and share expertise

Work across sectors

Microsoft

Florian Pennings
Director Government Affairs, Microsoft

Florian.pennings@microsoft.com