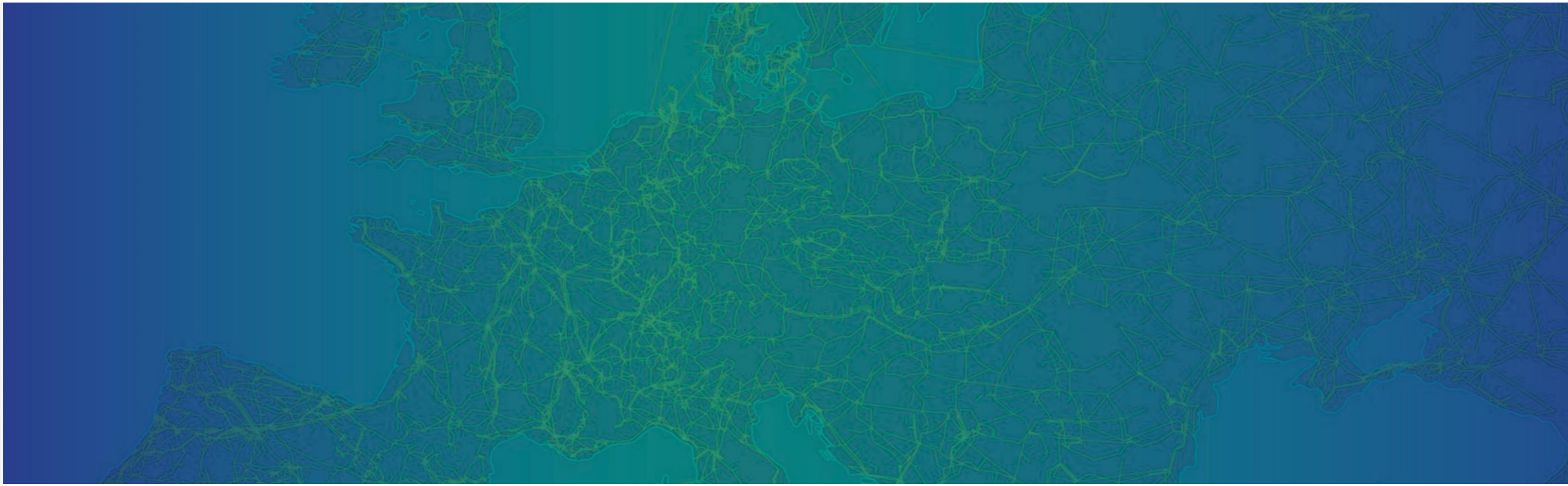
# Network Code on Cybersecurity

8 December 2023| UPES Conference | Tomas Šumskas



entsoe

Reliable Sustainable Connected

# Tomas Šumskas

- ENTSO-E Legal Manager for IT, Data, Contracts & Innovation
- 12 years experience in energy sector
- 7 years at ENTSO-E (European Network of Transmission System Operators for Electricity)
- 3 years Cybersecurity Network Code development team member

# What are the Network Codes?

- A set of rules applying to one aspect of energy sector
- NCs are regulations adopted by the Commission
- Legally binding in EU
- Introduced by Third Energy Package

# Network Codes

Codes adopted based on Third Energy Package

## Connection Codes:

- RFG
- DCC
- HVDC

## Market Codes:

- CACM
- FCA
- EBGL

## System Operation:

- SOGL
- ER

# New Cybersecurity Network Code (NCCS)

This Regulation establishes a network code which lays down sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

Applicable to all the EU countries.

# Cybersecurity Network Code (NCCS)

NCCS aims at:

- development of the cybersecurity risk assessment methodologies
- development of the cross-border electricity cybersecurity risk assessment report
- development of the common electricity cybersecurity framework
- development of the cybersecurity procurement recommendation
- development of the cybersecurity incidents classification scale methodology
- performance of the Union-wide cybersecurity risk assessment
- performance of the regional cybersecurity risk assessments
- definition of the regional cybersecurity risk treatment plans
- development of guidance on European cybersecurity certification schemes for ICT products, ICT services, and ICT processes
- development of guidelines for the implementation of this Regulation
- development of the transitional cybersecurity provisions

# Cybersecurity Network Code (NCCS)

- The Cyber Security Network Code is not the 1st Network Code **BUT** it is the 1st Network Code:
  - drafted according to the new Clean Energy Package rules
  - (co)drafted by ENTSO-E and EU DSO Entity
  - drafted in less than 6 months (!)
  - very diverse bodies and undertakings involved (energy and cybersecurity)
  - new governance (includes EU DSO Entity and all responsible bodies).
  - that is to be drafted when some of the main legislation on cyber security is under revision (e.g. NIS 2.0 Directive)

→ Many challenges tackled at once in the network code development phase.

# Cybersecurity Network Code (NCCS)

Responsibilities of very diverse bodies:

**EU Level:**

- ENTSO-E
- EU DSO entity (new)
- ACER
- ENISA
- NEMOs

**Regional Level:**

- Regional Coordination Centers (new)

**National Level:**

- National Regulatory Authorities (NRAs)
- National Competent Authorities (NCAs)
- NIS Competent Authorities
- Competent Authorities for Risk Preparedness (RP-NCAs)
- Competent Authorities Responsible for Cybersecurity (CS-NCAs)
- Computer Security Incident Response Teams (CSIRTs)

The code shall apply to all high-impact entities and critical-impact entities.

# Cybersecurity Network Code (NCCS)

## Application in non-EU Countries:

**Article 2.3 of the draft NCCS**
NCCS also apply to all entities who are not established in the Union but who deliver services to entities in the Union, provided they have been identified as high and critical-impact entities.

**Article 14 of the draft NCCS**
Requires certain TSOs to endeavour concluding agreements with the 3rd country TSO(s) that are neighbouring their SOR.
The concerned EU TSOs have 18 months to strive for an agreement with the relevant third country TSO(s).

# NCCS: Key Timelines

**14th of January 2022: NCCS proposal submitted to ACER**

*by* ENTSO-E & EU DSO Entity

**14th of July 2022: NCCS reviewed version submitted to the EC**

*by* ACER

**Q1 2024: Entry into force**

*by EC*

**2032? Final implementation**

*by specified entities*

# Thank you