Policy response for cybersecurity standardisation

Dr. Andreas Mitrakas
Head of Unit, "Market, Certification & Standardisation"

Cybersecurity Standardisation Conference 2022, Brussels and Online

15 │ 03 │ 2021
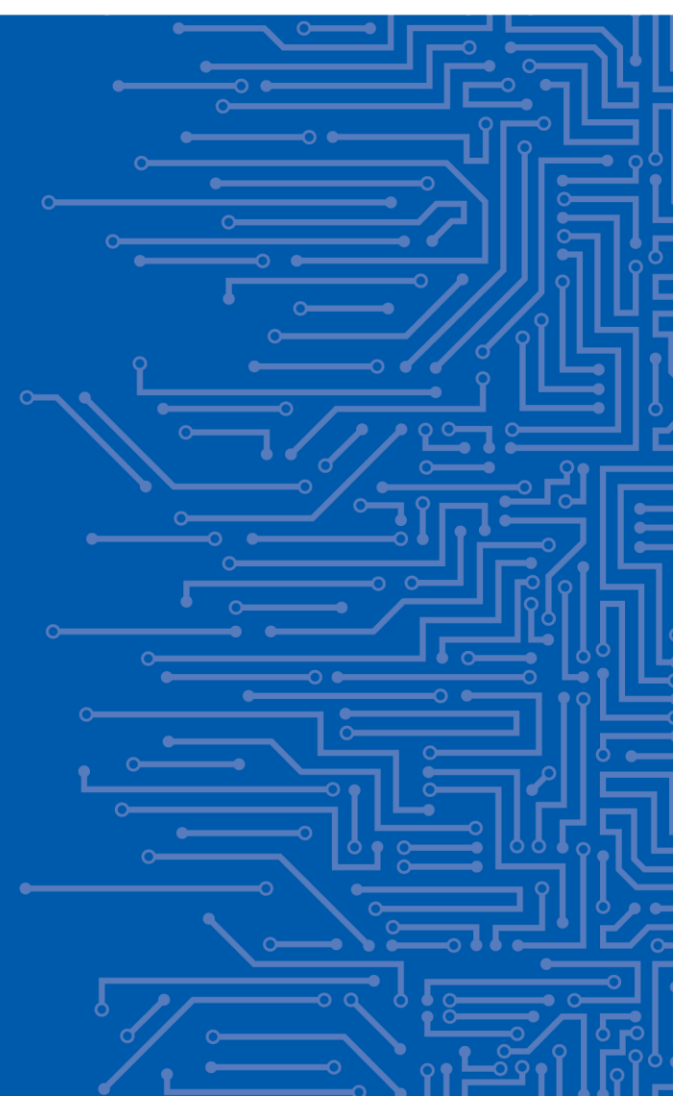
Agenda

Dynamic approach to standardisation

Developing policy requirements

Adapting policy responses

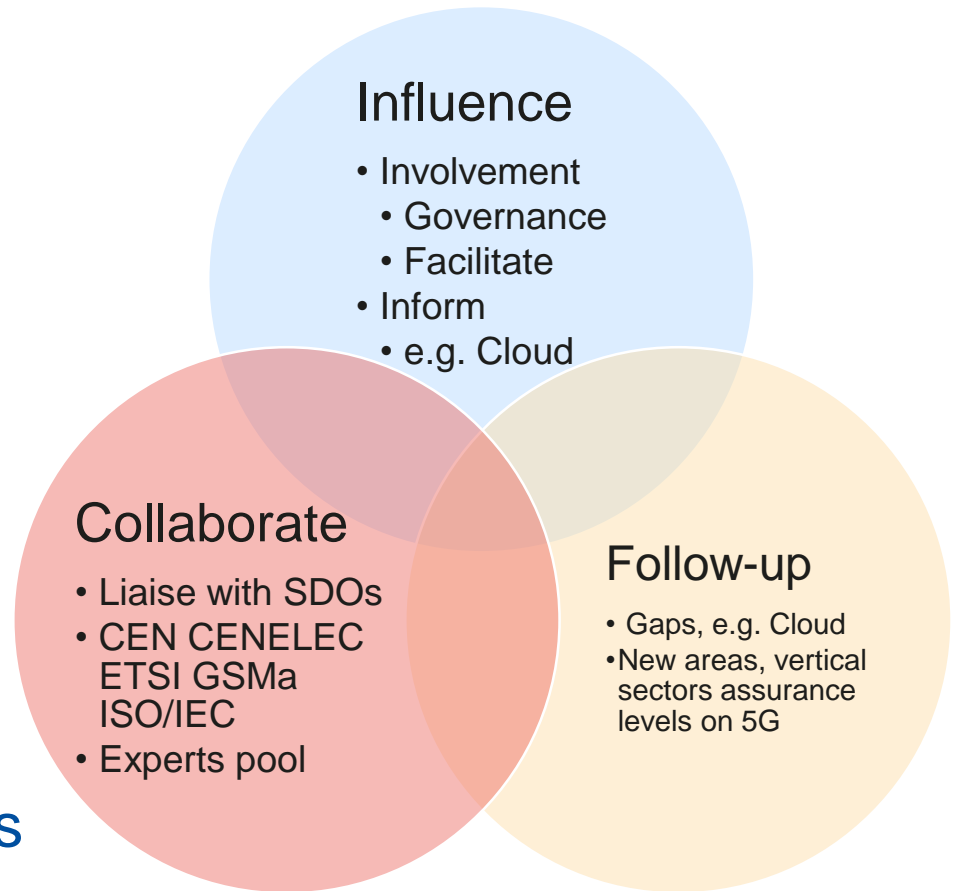# Dynamic approach to standardisation

Influence stakeholders

on key policy areas including cybersecurity certification

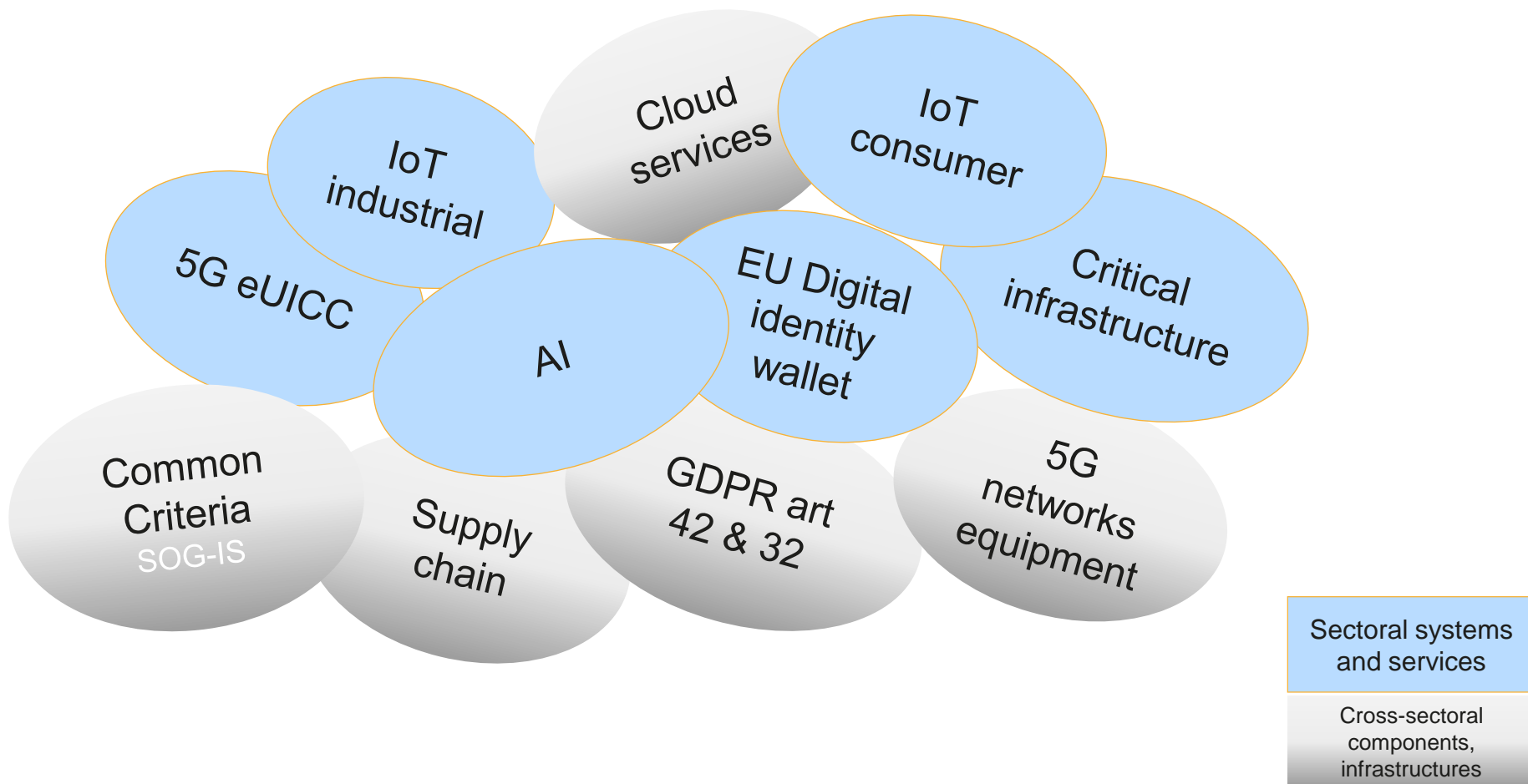**Collaborate with public interest and private stakeholders**

on the use and development of standards

Following up

On gaps and new content areas e.g. assurance level methodology

Influence
- Involvement
  - Governance
  - Facilitate
- Inform
  - e.g. Cloud

Collaborate
- Liaise with SDOs
- CEN CENELEC ETSI GSMa ISO/IEC
- Experts pool

Follow-up
- Gaps, e.g. Cloud
- New areas, vertical sectors assurance levels on 5G

enisa

Policy changes…

- 5G eUICC
- IoT industrial
- Cloud services
- IoT consumer
- Critical infrastructure
- AI
- EU Digital identity wallet
- Common Criteria SOG-IS
- Supply chain
- GDPR art 42 & 32
- 5G networks equipment

Sectoral systems and services

Cross-sectoral components, infrastructures

enisa

… and likely policy responses

Support the Commission at the strategic EU standardisation level bringing with cross-policy cybersecurity insight

Develop relations with MS standardisation organisations

Collaborate on knowledge management and training on cybersecurity standardisation as well as proactively pursue innovation goals with ECCC

Assist in translating legal requirements e.g. Rule of Law, to technical and organisational ones

THANK YOU FOR YOUR ATTENTION

📱 +30 28 14 40 9711

✉️ info@enisa.europa.eu

🌐 www.enisa.europe.eu