European Standardization Organizations

AI and Cybersecurity

Two sides of the same coin: trustworthiness in the digital space

Patrick Bezombes, co-chair CEN-CENELEC AI Focus Group

CEN-CENELEC in AI standardization

- CEN-CENELEC AI Focus Group
  - Launched in 2019 – Final report in 09/2020 (AI Roadmap available on CEN-CLC website)
  - Transitioning towards a CEN-CENELEC 'AI and data' Joint Technical Committee (JTC)
  - Considering strong interactions with ETSI

- CEN-CENELEC future JTC will work closely with ISO/IEC JTC 1 SC 42:
  - Liaisons with SC 42 - many cross-participations anticipated
  - Most SC 42 standards will constitute the basis of EU standards and will be endorsed
  - Potential European initiatives when it comes to safety, ethics, sovereignty – security?

- Regular exchanges with the European Commission
  - Mapping existing (and future) International standards against EU policy
  - Alignment between AI regulations and AI standardization needs to be addressed

Future certification scheme shall rely on available and future European and International Standards

Future JTC scope

- Multiple dimensions to be addressed:
  - Concept and terminology
  - Technical
  - Societal/ethical
  - AI and data governance
  - Interoperability
  - Securing AI and data (?)

- Challenges:
  - Fragmentation of AI standardisation activities with a trend to proliferation and overlapping
  - Highly-competent EU third parties (ENISA-like) needed for certification
  - Cooperation between relevant parties – anticipation

Key issues for AI standardization

- Neural network (deep learning) robustness
  - **Explainability**: R&D still needed
  - Importance to start **pre-standardization work**

- Encoding fairness, ethics…
  - How to specify and assess?
  - Regional characteristics

- How to address "Threats" coming from the environment ➔ wrong predictions / wrong decisions

- **AI systems certification schemes** (i.e. for safety critical systems operating in open environment)
  - Use of simulation for design, validation, certification and even accident investigation
  - Simulation will rely on:
    - Digital twins of the AI systems (➔ certification of the digital twins?)
    - Models of the operating environment (➔ specification and certification of the models?)

Certifications schemes will be key to safety and security and at the core of the European AI legal framework

Connecting AI and Cybersecurity

- Intertwined technologies :
  - AI technologies will be used in cybersecurity
  - Cybersecurity will be used to protect AI & data spaces

<u>the data that feeds AI systems needs to be secured</u>

- A strong need of « Cybersecurity » expertise for countering the threats on AI and data :
  - Terminology and concepts : authenticity, integrity, traceability, identity….
  - Methodology…

<u>Moving from « Trusted AI » to a « Trusted AI ecosystem » concept</u>

Holistic Trustworthiness approach needed covering cloud, IoT, computing, Data, AI…

Digital sovereignty: impacts on AI and Cybersecurity

Digital sovereignty ("DS") requirements may lead to the creation of new sets of standards supporting:

- ✓ Digital identity
- ✓ Digital ownership
- ✓ Digital law enforcement
- ✓ Digital jurisdiction
- ✓ Digital territory…

- ❑ needs to better understand "DS" in order to anticipate future standardization requirements.
- ❑ **needs to tackle "DS" at European level to avoid national bias.**

Dynamic link with International Standardization in ISO and IEC

Invite ENISA, CEN-CLC/JTC 13, CLC/TC 65X, ETSI TC CYBER and all experts to contribute to the CEN-CENELEC AI standardization activities