Telecom Industry Perspective on AI Properties and Human Aspects
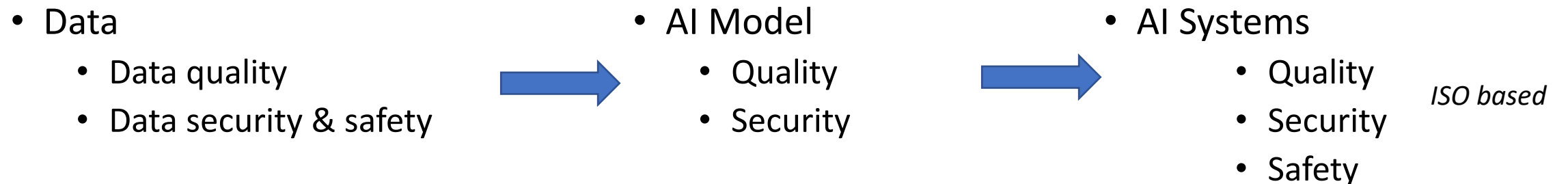
Ewelina Szczekocka

ENISA
AI CYBERSECURITY CONFERENCE

7 June, Brussels

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

orange™
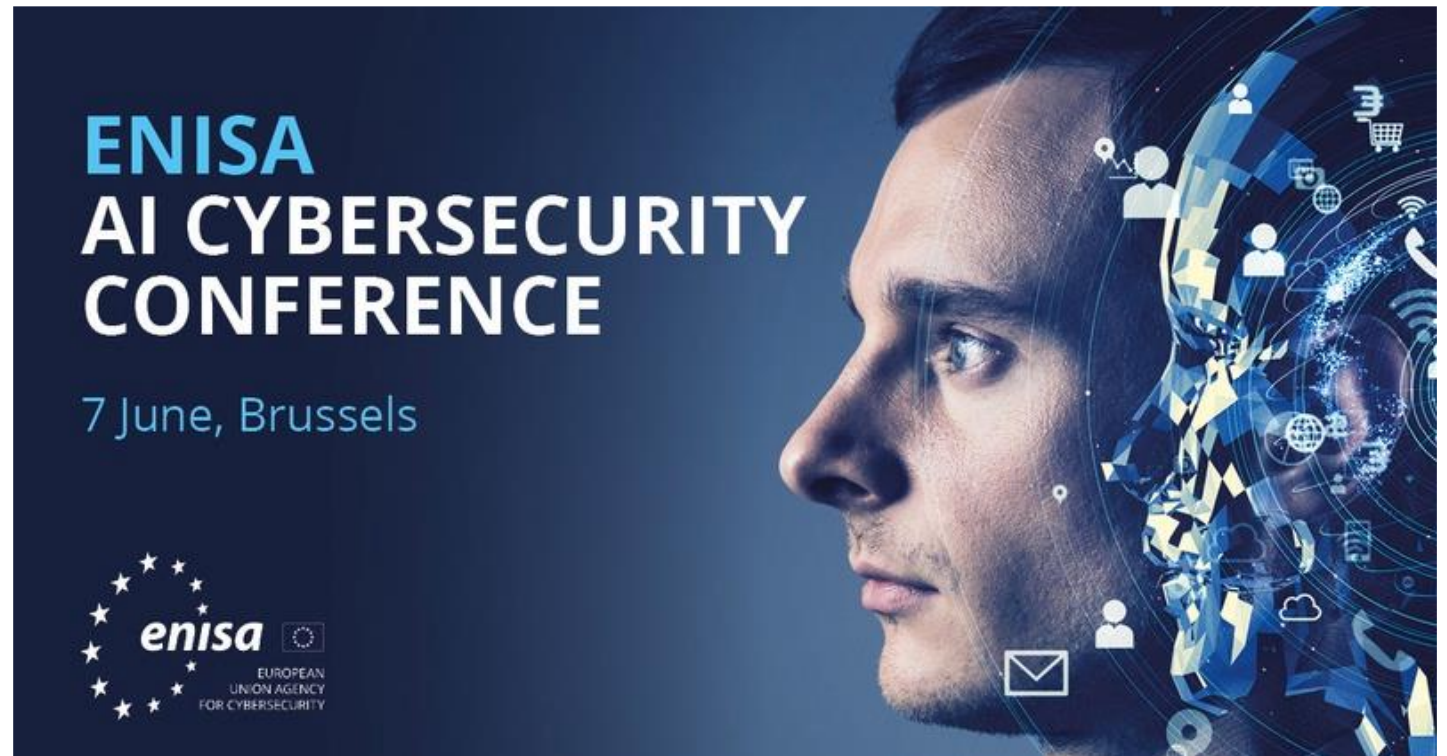
Context of AI Cybersecurity for Industry

- AI as a multifaceted approach with different aspects: IT, legal, business, social
- AI introduces many challenges (risks and opportunities)
- Regulations in EU under construction: AI Act, Cyber Resilience Act
- Engagement of different stakeholders (impacting and impacted by AI)

- AI Cybersecurity one of the key challenges
- Practical need of AI benchmarking and appropriate metrics for Industry
- Goal: to develop AI systems complying with the conformity rules, trustworthy
- AI Risk Management, Quality of AI systems

- Data
  - Data quality
  - Data security & safety

→

- AI Model
  - Quality
  - Security

→

- AI Systems
  - Quality
 - Security
  - Safety

ISO based

AI Properties in Telecommunication

- AI in telco: **network optimization** (e.g., automate optimization of network quality), **predictive maintenance** (e.g., detecting potential failures, load balancing), customer scoring, **AI functionalities for services** (e.g., computer vision for worker safety, personalisation....)

Example: Use Cases

AI Properties	Load balancing	Customer scoring
Robustness	high	high
Fairness	<analysed>	critical
Transparency	high	critical
Availability	critical	low
Integrity	critical	critical
Confidentiality	high	critical

AI Benchmarking – tools across AI life cycles
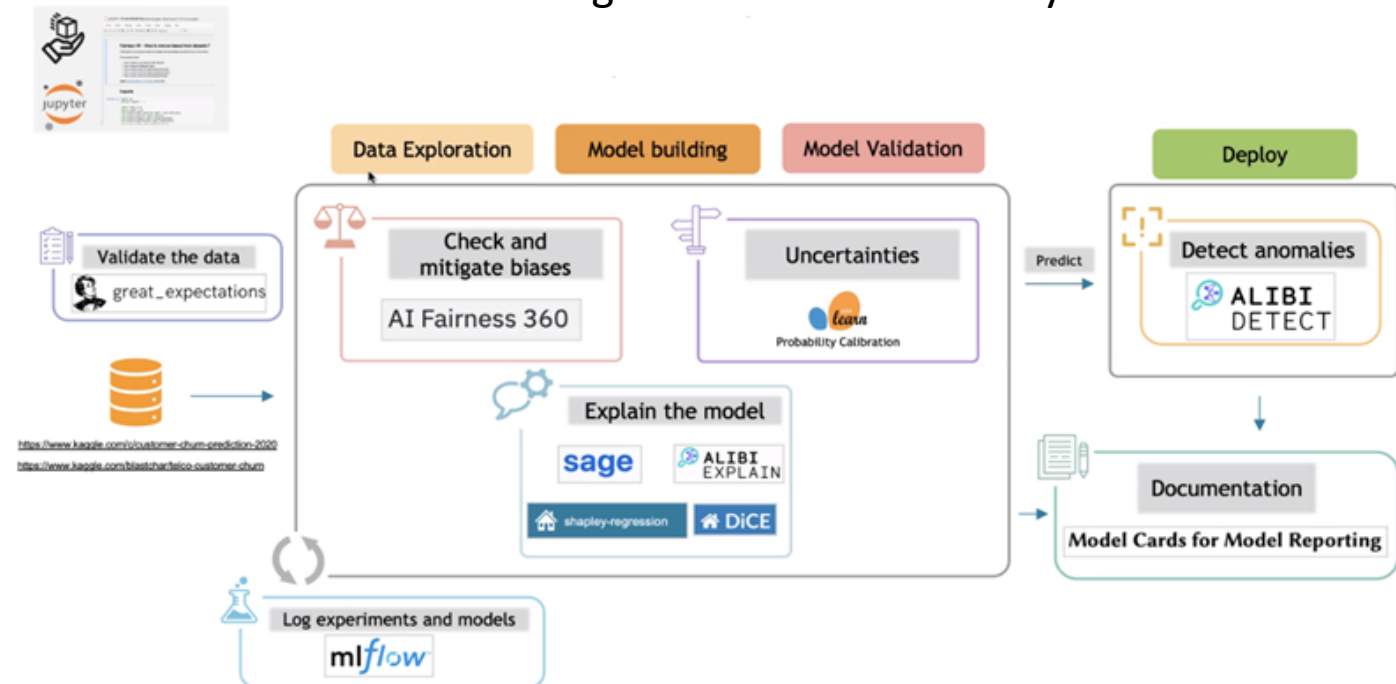
AI Human Aspects

- European Convention of Human Rights (Council of Europe)
- Charter of Fundamental Rights (EC)
- Use cases concerned with network: no personal data used, based on traffic aggregates (aspects related to fairness might occur e.g., for geographic regions, devices), aspects of human oversight (in the case of full automation)
- Use cases concerned with customer: personal data used, profiling aspects
- Bias in data, bias in models, … (ex. ISO fairness metrics, e.g., equality of odds, parity, …)

Harm to People	Harm to an Organization	Harm to an Ecosystem
• Individual: Harm to a person's civil liberties, rights, physical or psychological safety, or economic opportunity.	• Harm to an organization's business operations.	• Harm to interconnected and interdependent elements and resources.
• Group/Community: Harm to a group such as discrimination against a population sub-group.	• Harm to an organization from security breaches or monetary loss.	• Harm to the global financial system, supply chain, or interrelated systems.
• Societal: Harm to democratic participation or educational access.	• Harm to an organization's reputation.	• Harm to natural resources, the environment, and planet.

Source: NIST

Thank You/Merci

Ewelina Szczekocka, Orange Innovation Poland

ewelina.szczekocka@orange.com

orange™