Addressing AI cybersecurity requirements

Henrik Junklewitz, Ronan Hamon, Ignacio Sanchez

European Commission Joint Research Centre (JRC)

ENISA AI Cybersecurity Conference 2023, Brussels

European Commission

JRC - Science for policy

ANTICIPATE

INTEGRATE

IMPACT

Our purpose

The **Joint Research Centre** provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society.

European Commission

AI Cybersecurity Certification – Requirements and Standards

certification of **security requirements**

Standards in AI Cybersecurity

- ISO 27000 series partially applicable to AI as a software
- International standards (ISO, CEN, ETSI…) in development,
- Early stages in the drafting process for harmonised European standards

Legal Requirements

- **AI Act: requirements on cybersecurity (Art. 15)** - other trustworthy requirements - presumption of conformity with standards (Article 42)
- CRA: software security baseline standards
- CSA: certification schemes

AI Cybersecurity Requirements – the AI Act

Addressing the cybersecurity of AI **in the context of the AI Act and expected European harmonised standards**

Cybersecurity-specific elements in the AI Act

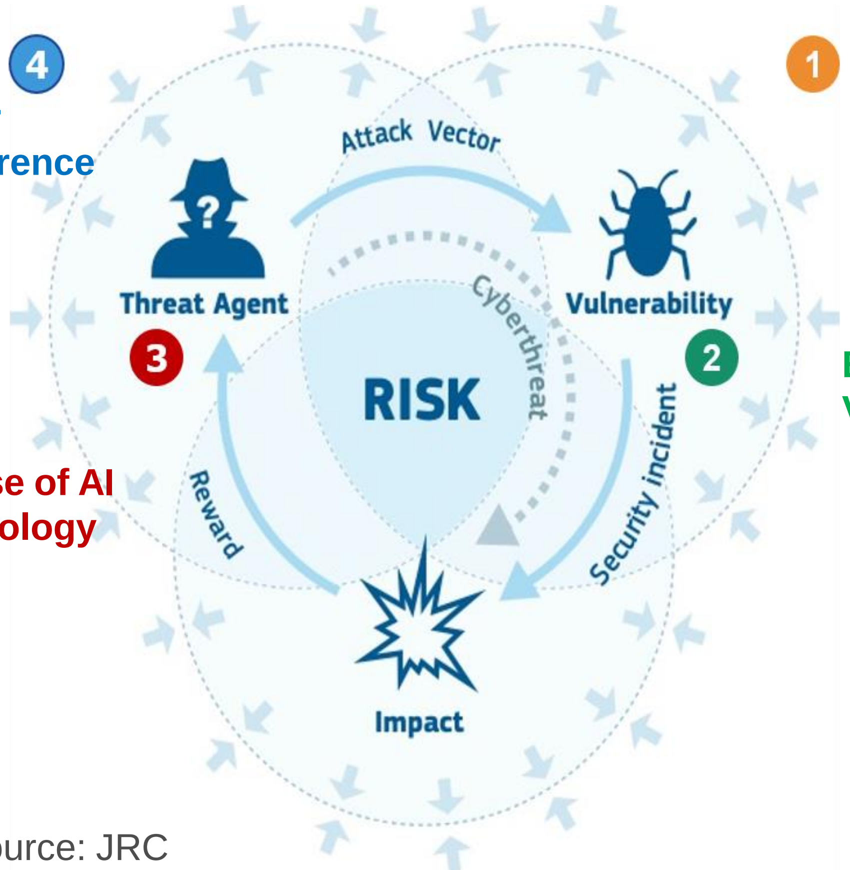
- Article 15 paragraph 4 on cybersecurity,
- Annex II 2.8 of standardisation request (SR)
- Integration of existing cybersecurity risk management approaches (recital 51, SR).
- Address AI and non-AI cybersecurity technological questions (e.g. adversarial machine learning)
- Connections with other EU regulations (GDPR, CRA, CSA)

Cybersecurity in the context of other trustworthiness requirements in the AI Act

- Most relevant requirements: risk (Art. 9), data (Art. 10), human oversight (Art. 14), conformity (Art.16)
- Laid down together with accuracy and robustness in (Art. 15)

European Commission

Technological challenges in AI Cybersecurity



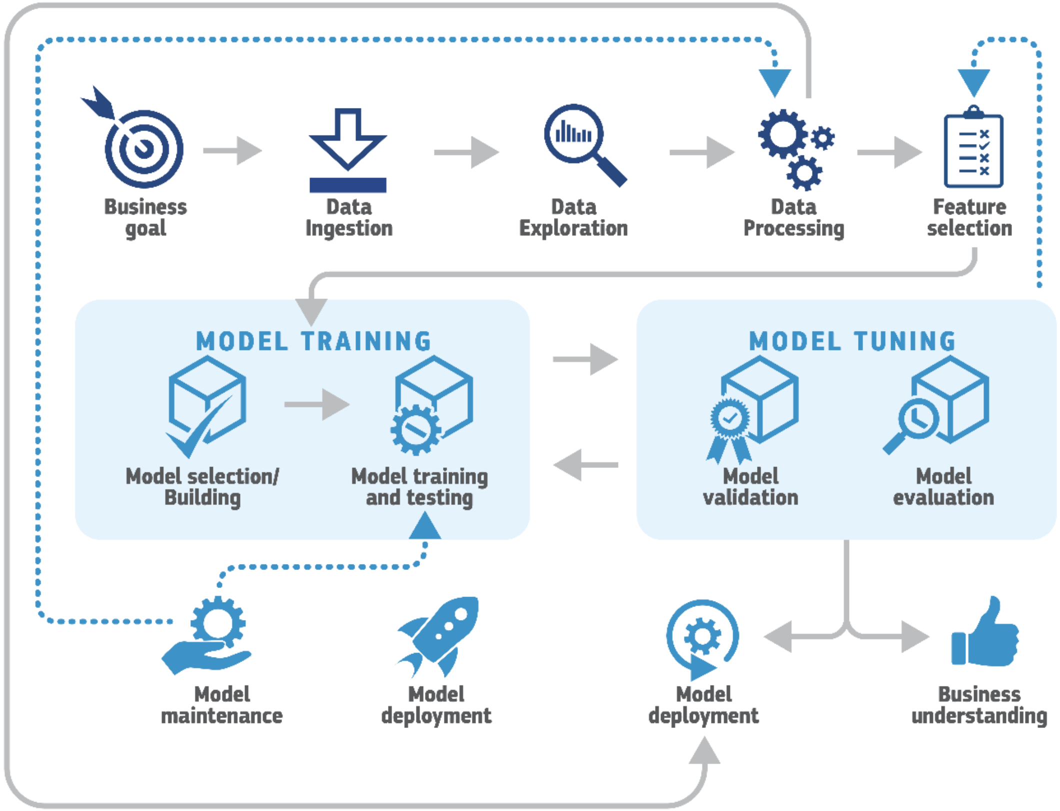
AI for deterrence

AI security: Mitigation and Control

Exploiting AI Vulnerabilities

Misuse of AI technology

Source: JRC



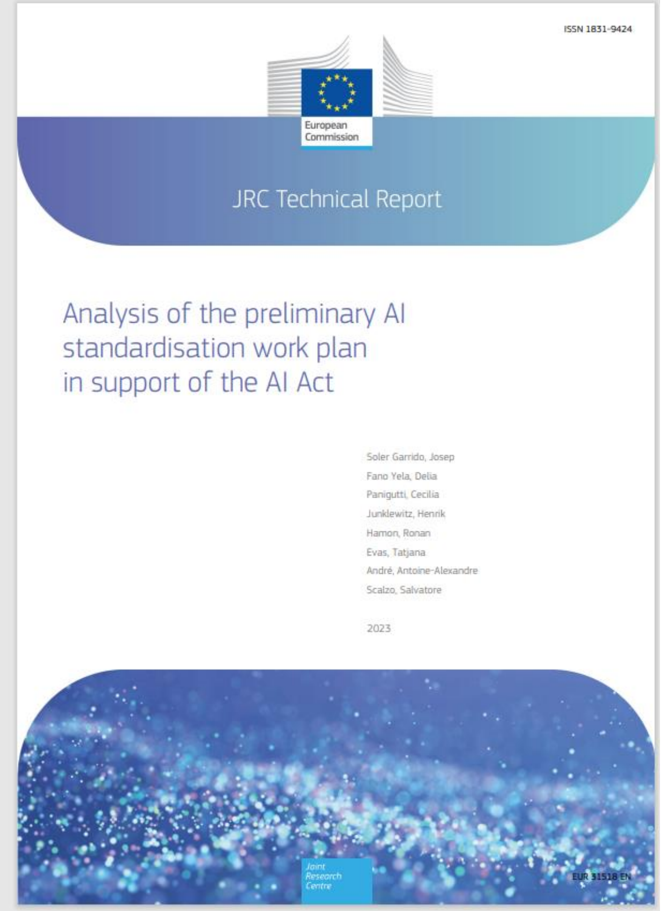
Source: JRC

Technological challenges in AI Cybersecurity

- Addressing model-specific adversarial attacks
- Integration of AI cybersecurity into AI lifecycle management
- Real world AI threat modelling experience
- Robustness measures and cybersecurity metrics for complex AI models
- AI-model-level mitigation measures and defences
- Known trade-offs between requirements (e.g. accuracy vs.adversarial robustness; transparency vs. cybersecurity)
- AI data and model supply chain security
- Preventing misuses of complex AI models
- …

State of Play in AI Cybersecurity Standardisation

Source: JRC; Stable Diffusion 1.4. Text prompt: "AI Cybersecurity Standardisation"



ISSN 1831-9424

European Commission

JRC Technical Report

Analysis of the preliminary AI
standardisation work plan
in support of the AI Act

Soler Garrido, Josep
Fano Yela, Delia
Panigutti, Cecilia
Junklewitz, Henrik
Hamon, Ronan
Evas, Tatjana
André, Antoine-Alexandre
Scalzo, Salvatore

2023

Joint
Research
Centre

EUR 31518 EN

[Analysis of the preliminary AI standardisation work plan in support of the AI Act - Publications Office of the EU (europa.eu)]

European
Commission

State of Play in AI Cybersecurity Standardisation

Source: JRC; Stable Diffusion 1.4. Text prompt: "AI Cybersecurity Standardisation"

- **Defined by the current AI state-of-the-art** (see EC standardisation request)
- **Non-AI-specific:** ISO 27000 series: should be **applicable to “AI-as-Software”** including security controls (27002) and risk management (27005), **but need adaptation.**
- **AI-specific:** growing number of taxonomies (NIST, MITRE, ENISA) and technical reports (ISO, ETSI); **international standards on AI-specific cybersecurity in development** (e.g. ISO 27090)

What to do in practice?

Source: JRC; Stable Diffusion 1.4. Text prompt: "AI Cybersecurity Standardisation"

I. **The focus of the AI Act is on AI systems.**

II. **Acknowledge limits in the technological state-of-the-art**

III. **Leverage AI- and non-AI security techniques depending on AI component model maturity.**

IV. **No size fits all – importance of risk based approach to cybersecurity.**

Thank you
and keep in touch

EU Science Hub
joint-research-centre.ec.europa.eu

- @EU_ScienceHub
- EU Science Hub – Joint Research Centre
- EU Science, Research and Innovation
- EU Science Hub
- @eu_science

European Commission