AI Security Standards

Evaluation and AI Governance

Workshop
8th of May, 2025
Warsaw, hybrid

NASK

NASK

Keeping the Internet Safe

Since 1993

Research & Innovation

AI Security Research Center

Exploring the safety and reliability of artificial intelligence.

Cybersecurity R&D Division

Developing advanced protection systems against cyber threats.

Cloud & Intelligent Networks Division

Researching secure IoT systems and quantum communication.

Science Development Office

Strengthening NASK’s role in national and international research initiatives.

Digital Transformation

EZD RP NASK

Modernizing public administration

A digital document management system integrated with ePUAP and e-Delivery.

OGÓLNOPOLSKA SIEĆ EDUKACYJNA ose NASK

Secure internet for schools

Providing free, high-speed, and safe internet access to all schools in Poland, along with educational resources.

blockchain NASK

Blockchain for public services

Leveraging blockchain technology to enhance security and trust in digital administration.

Certification NASK

Raising quality and security standards

Evaluation and Certification of products, processes, services and qualification.

Online Safety

Standing against cybercriminals

National level **CSIRT**

Removing illegal content

Efforts focus on eliminating child sexual abuse materials and harmful content.

Reports help accelerate the removal process.

Disinformation Analysis Center – Identifying misinformation

Disinformation campaigns are monitored and analyzed to provide timely warnings.

Education & Digital Awareness

cyber profilaktyka NASK

Cyber Awareness Programs

Educational initiatives such as Cyber Lessons 3.0, Make It Clear, and Safer Internet promote safe and responsible internet use among children and young people.

.pl NASK

.pl Domain Registry Management

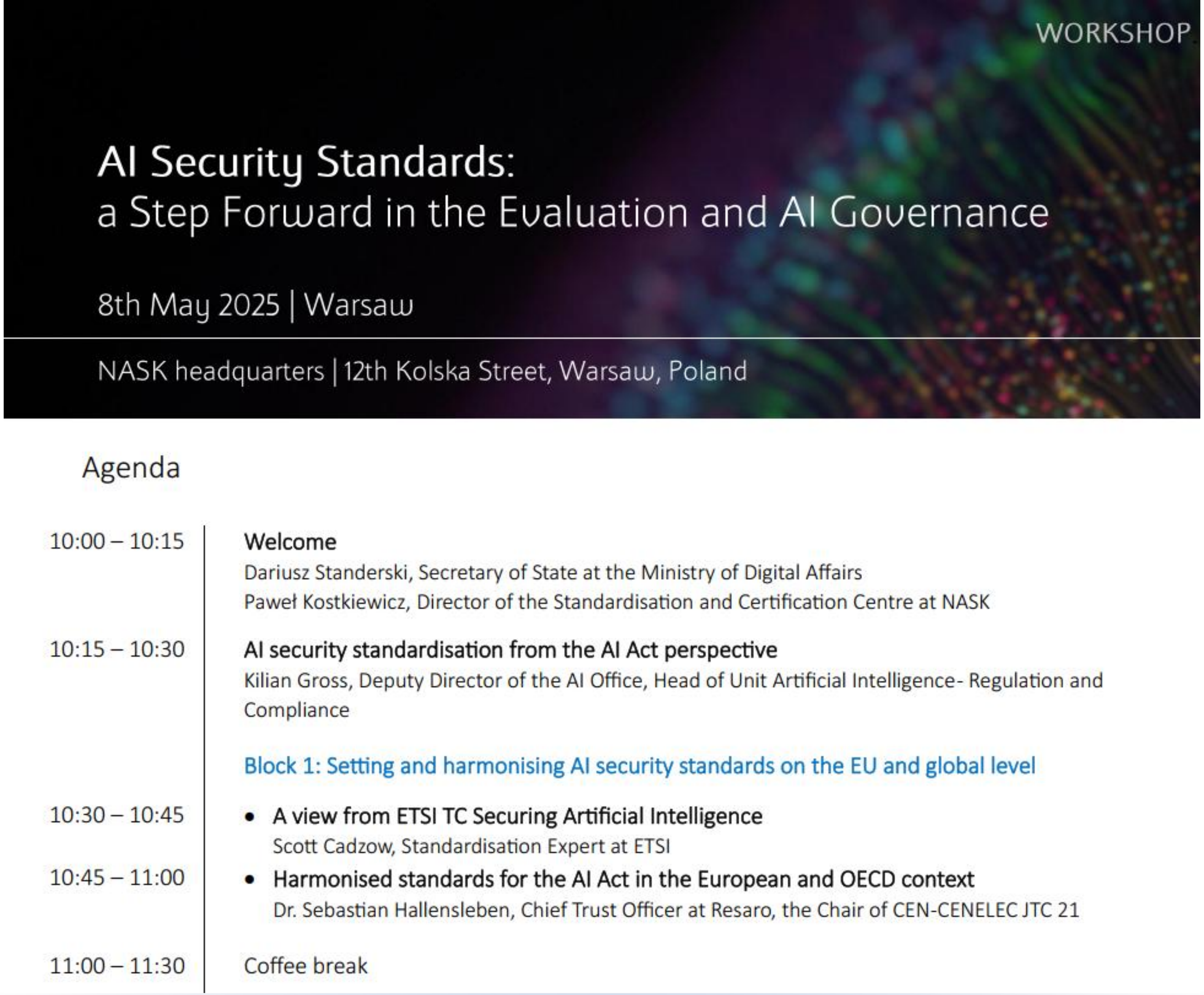
The .pl domain registry is maintained in partnership with accredited registrars as part of the NASK Partner Program.

ESA NASK

Educational Anti-Smog Network

Air quality monitoring combined with educational resources helps raise awareness of environmental issues.

The purpose of the workshop is to share knowledge on AI security standards developments among experts and all interested parties.



WORKSHOP

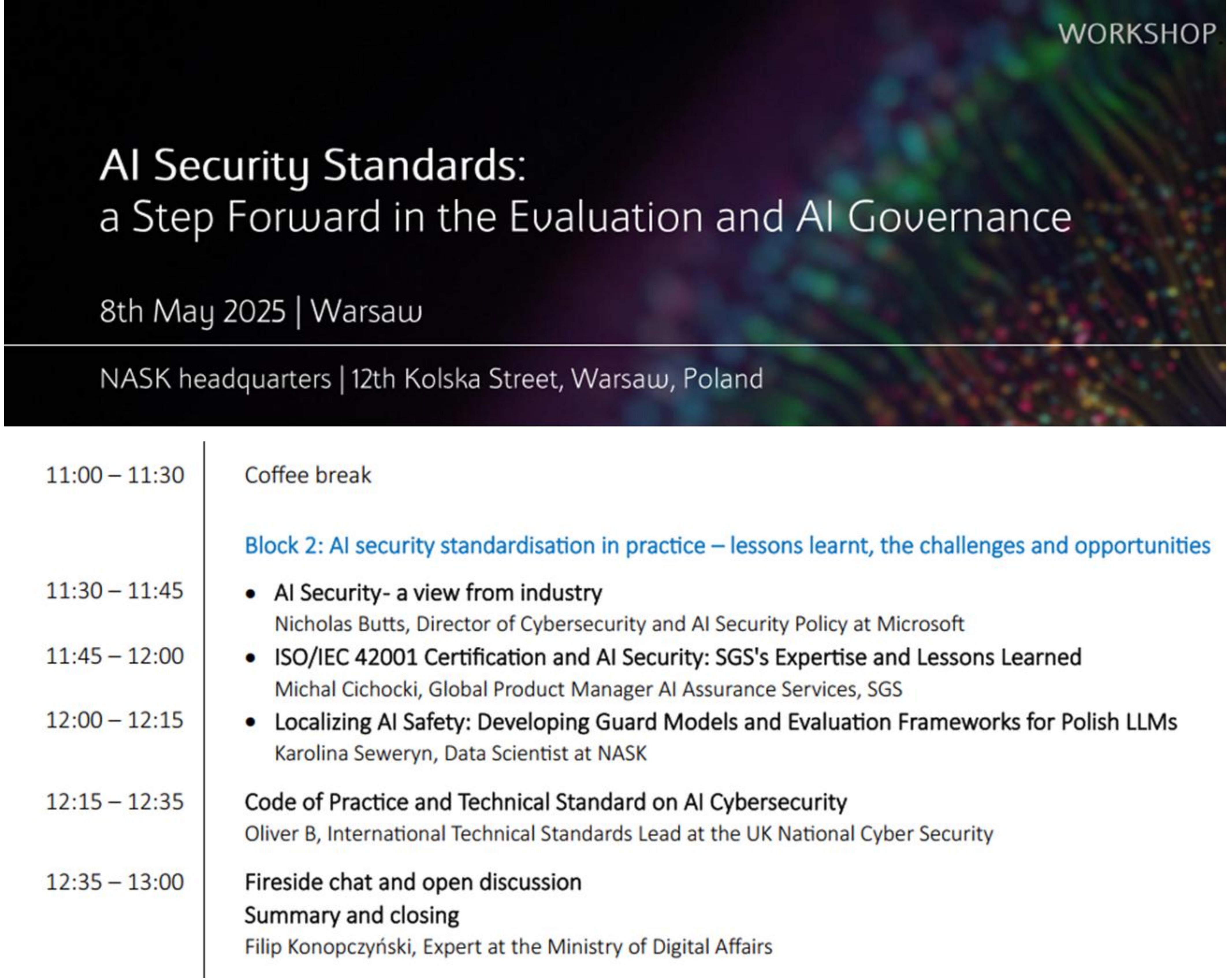
AI Security Standards: a Step Forward in the Evaluation and AI Governance

8th May 2025 | Warsaw

NASK headquarters | 12th Kolska Street, Warsaw, Poland

Agenda

10:00 – 10:15	**Welcome** Dariusz Standerski, Secretary of State at the Ministry of Digital Affairs Paweł Kostkiewicz, Director of the Standardisation and Certification Centre at NASK
10:15 – 10:30	**AI security standardisation from the AI Act perspective** Kilian Gross, Deputy Director of the AI Office, Head of Unit Artificial Intelligence- Regulation and Compliance
	Block 1: Setting and harmonising AI security standards on the EU and global level
10:30 – 10:45	• **A view from ETSI TC Securing Artificial Intelligence** Scott Cadzow, Standardisation Expert at ETSI
10:45 – 11:00	• **Harmonised standards for the AI Act in the European and OECD context** Dr. Sebastian Hallensleben, Chief Trust Officer at Resaro, the Chair of CEN-CENELEC JTC 21
11:00 – 11:30	Coffee break



WORKSHOP

AI Security Standards:
a Step Forward in the Evaluation and AI Governance

8th May 2025 | Warsaw

NASK headquarters | 12th Kolska Street, Warsaw, Poland

11:00 – 11:30 Coffee break

Block 2: AI security standardisation in practice – lessons learnt, the challenges and opportunities

11:30 – 11:45
- **AI Security- a view from industry**
  Nicholas Butts, Director of Cybersecurity and AI Security Policy at Microsoft

11:45 – 12:00
- **ISO/IEC 42001 Certification and AI Security: SGS's Expertise and Lessons Learned**
  Michal Cichocki, Global Product Manager AI Assurance Services, SGS

12:00 – 12:15
- **Localizing AI Safety: Developing Guard Models and Evaluation Frameworks for Polish LLMs**
  Karolina Seweryn, Data Scientist at NASK

12:15 – 12:35 **Code of Practice and Technical Standard on AI Cybersecurity**
Oliver B, International Technical Standards Lead at the UK National Cyber Security

12:35 – 13:00 **Fireside chat and open discussion**
Summary and closing
Filip Konopczyński, Expert at the Ministry of Digital Affairs

Enjoy!