Council of the European Union
General Secretariat

Brussels, 10 June 2024

WK 8348/2024 INIT

LIMITE

JAI
FRONT

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Frontiers
Subject:	Artificial Intelligence in Migration and Home Affairs

Delegations will find attached the presentation made by the Commission at the meeting of the Working Party on Frontiers of 06 June 2024 on the above-mentioned subject.

Artificial Intelligence in Migration and Home Affairs

Political agreement on the AI Act and implications for border management

Unit F2. DG Home Affairs and Migration

AI in Border Management

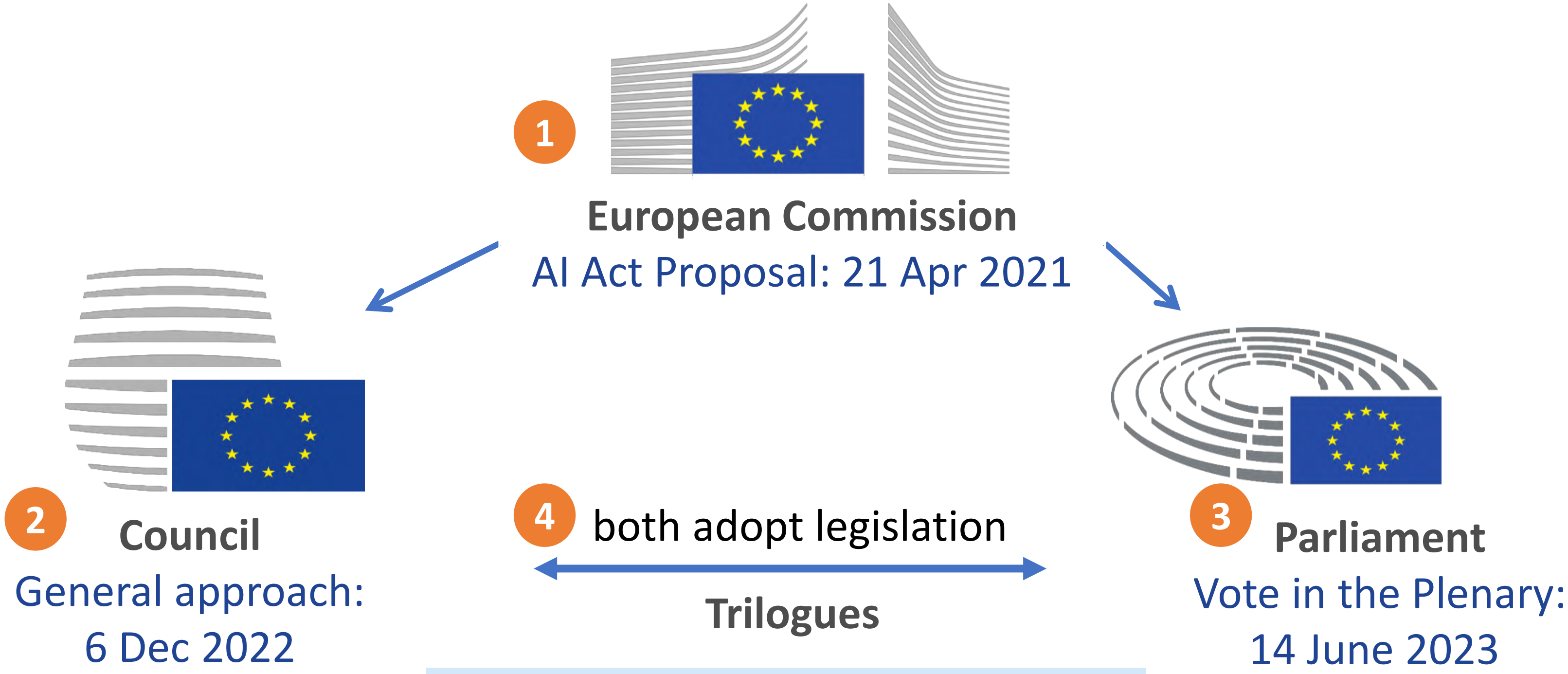
Examples of possible AI use cases in the management of borders

- Large-scale IT systems, incl. biometric technologies (e.g. automated fingerprint and face recognition)
- Automated Border Control (ABC)
- Monitoring, analysis and forecasting of migration flows;
- Risk assessment and screening e.g. identifying unknown persons of interest based on specific data-based risk profiles, such as individuals posing a security risk or risk of irregular migration
- Interacting with clients- e.g. language translation, chatbots in various languages to offer on-the spot assistance;
- Tools such as small unmanned aerial systems
- Object recognition
- Geospatial data analytics

Political agreement on the European AI Act

European
Commission

A political agreement on the EU AI Act was reached



1 **European Commission**

AI Act Proposal: 21 Apr 2021

2 **Council**

General approach:
6 Dec 2022

3 **Parliament**

Vote in the Plenary:
14 June 2023

4 both adopt legislation

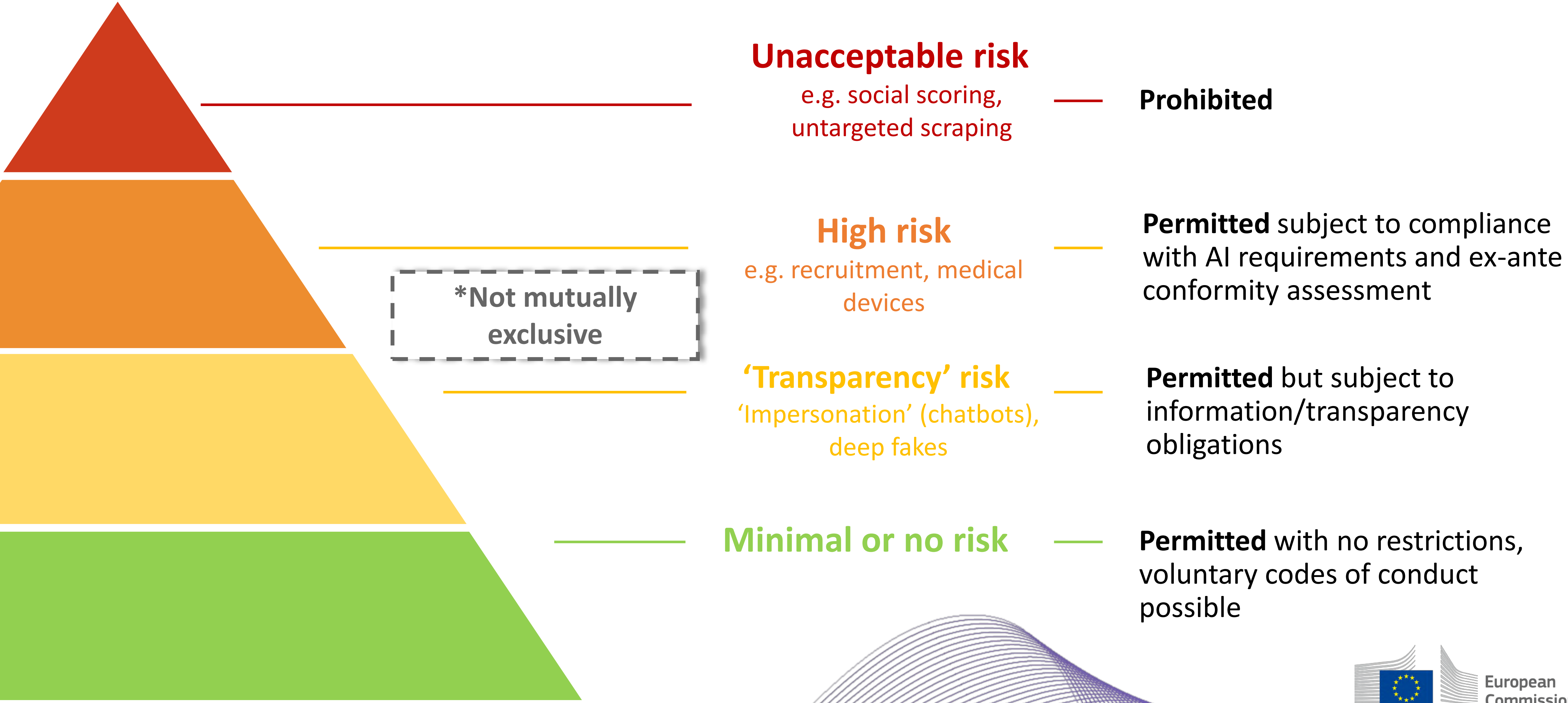
Trilogues

On 8 Dec 2023
a political agreement was reached

The first comprehensive legislative framework for AI in the world.
It ensures that Europeans can trust what AI has to offer.

DIGITAL COMMISSION ESSENTIALS
Easy, quick, for everyone

The AI Act follows a risk-based approach



*Not mutually exclusive

Unacceptable risk
e.g. social scoring, untargeted scraping — **Prohibited**

High risk
e.g. recruitment, medical devices — **Permitted** subject to compliance with AI requirements and ex-ante conformity assessment

'Transparency' risk
'Impersonation' (chatbots), deep fakes — **Permitted** but subject to information/transparency obligations

Minimal or no risk — **Permitted** with no restrictions, voluntary codes of conduct possible

A limited set of particularly harmful AI practices are banned

Unacceptable risk

Subliminal, manipulative techniques or exploitation of vulnerabilities	to manipulate people in harmful ways
Social Scoring	for public and private purposes leading to detrimental or unfavourable treatment
Biometric categorisation	to deduce or infer race, political opinions, religious or philosophical beliefs or sexual orientation, exceptions for labelling in the area of law enforcement
Real-time remote biometric identification	In publicly accessible spaces for law enforcement purposes, -with narrow exceptions and with prior authorisation by a judicial or independent administrative authority
Individual predictive policing	assessing or predicting the risks of a natural person to commit a criminal offence based solely on this profiling without objective facts
Emotion recognition	in the workplace and education institutions, unless for medical or safety reasons
Untargeted scraping of the internet	or CCTV for facial images to build-up or expand biometric databases

Remote Biometric Identification- further detail

Real-time remote biometric identification-

Prohibited from use in publicly accessible spaces for law enforcement purposes with limited exceptions:

i) Targeted searches for specific victims of abduction, trafficking in human beings and sexual exploitation, as well as searches for missing persons;

ii) Prevention of threat to life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

iii) Localisation or identification of a person suspected of committing a criminal offence, for the purpose of conducting a criminal investigation, prosecution or executing a criminal penalty for offences, referred to in Annex IIa of the Regulation and punishable by a maximum period of at least four years imprisonment.

Safeguards: fundamental rights impact assessment & registration of the tool in EU database + 'High-risk' obligations + prior authorisation + notification to the market surveillance authority and DPA.

Post-remote biometric identification-

Not prohibited but considered '**high-risk'.**

Safeguards: 'high-risk' obligations + prior authorisation + must only be used in a targeted manner in cases of present or genuine foreseeable threat of criminal offence or search for specific missing persons.

High-risk AI systems will have to comply with certain rules

1. High-risk systems embedded in products covered by Annex II

2. High-risk (stand-alone) use cases listed in Annex III:

- **Biometrics:** Remote biometric identification, categorization, emotion recognition;
- **Critical infrastructures**: e.g. safety components of digital infrastructure, road traffic
- **Education**: e.g. to evaluate learning outcomes, assign students in educational institutions
- **Employment:** e.g. to analyse job applications or evaluate candidates, promote or fire workers
- **Essential private and public services**: determining eligibility to essential public benefits and services; credit-scoring and creditworthiness assessment, risk assessment and pricing in health and life insurance
- **Law enforcement:** e.g. assess risk of persons committing a crime, emotion recognition, biometric categorization, profiling of persons in the context of an investigation
- **Border management:** e.g. assess risk of irregular migration of a person entering a MS, assess visa, residence permit application and associated complaints
- **Administration of justice and democratic processes**

Filter mechanism: Excludes systems from the high-risk list that:

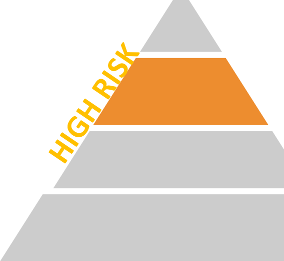
- perform narrow procedural tasks,
- improve the result of previous human activities,
- do not influence human decisions or
- do purely preparatory tasks,

NB. Profiling of natural persons always high-risk

High-risk AI systems JHA use cases Listed in Annex III

- **Biometric use cases:**
  - Real-time biometric identification is prohibited with strict exceptions under high risk + additional safeguards
  - Post-remote biometric identification added to high risk + additional safeguards
  - Biometric categorization of sensitive or protected attributes or characteristics
  - AI systems intended for emotion recognition
- **Law enforcement:**
  - AI systems intended to assess the risk of a natural person becoming a victim of a criminal offence
  - AI systems used to assess the risk of a person (re)offending- cannot be based solely on profiling or on personality traits or past criminal behaviour
  - AI systems used as polygraphs
  - AI systems utilized to evaluate reliability of evidence in investigation or prosecution
  - AI system for profiling of natural persons in detection, investigation or prosecution of criminal offences
- **Migration, asylum and Border management:**
  - AI systems used as polygraphs
  - AI systems intended to assess a risk of security, irregular migration, or health posed by a natural person intending to enter a MS
  - AI systems used to examine applications for asylum, visa & residence permits and associated complaints on eligibility
  - AI systems used to detect, recognize or identify natural persons. **This excludes verification of travel documents!**

Obligations of providers and deployers of high-risk AI



Provider obligations

- **Risk management system** to minimise risks for deployers and affected persons
- **Trustworthy AI requirements:** data quality and management, documentation and traceability, transparency and information to deployers, human oversight, accuracy, cybersecurity and robustness
- **Conformity assessment** to demonstrate compliance prior to placing on the market
- **Quality management system**
- **Register** standalone AI system in EU database (listed in Annex III)
- Conduct **post-market monitoring** and report **serious incidents**
- Non-EU providers to appoint **authorized representative in the EU**

Deployer obligations

- Operate high-risk AI system in accordance with **instructions of use**
- Ensure **human oversight**: persons assigned must have the necessary competence, training and authority
Monitor for possible risks and **report problems and any serious incident** to the provider or distributor
- Public authorities to **register the use in the EU database**
- **Inform affected workers** and their representatives
- **Inform people an explanation** subjected to decisions taken or informed by a high risk AI system and, upon request, provide them with

The impact on fundamental rights has to be assessed

The use of a high-risk AI system may produce an impact on fundamental rights after deployement
Prior to first use, some deployers must do a **fundamental rights impact assessment for Annex III systems** (except critical infrastructure)

Consisting of an assessment of:

► **Deployers' processes**, in which the high-risk AI system is intended to be used

► **Categories of natural persons and groups** likely to be affected by its use in the specific context

► **Specific risks of harm** likely to impact the affected categories of persons or group of persons

►Description of **human oversight measures**

►Measures to be taken **in case of materialization of the risks**

Carried out by

Deployers that are

1. Bodies governed by **public law**
2. Private operators providing **public services**
3. Certain other **private providers** (credit scoring/ credit worthiness assessment of health and life insurances)

Rules for AI systems which are not high-risk

Transparency obligations for certain AI systems (Art. 52)

- **Notify humans** that they are **interacting with an AI system** unless this is evident
- Design **generative AI** so that synthetic audio, image, video or text content **is marked in a machine readable format and detectable as artificially generated**
- Deployers to **label as artificially generated:**
  - **deep fakes** (audio, image or video unauthentic content)
  - **text** if published with the purpose of informing the public on matters of public interest
- Notify humans that **emotion recognition or biometric categorisation systems** are applied to them

Possible voluntary codes of conduct (Art. 69)

- No mandatory obligations, but possibility for voluntary application of the AI Act requirements to non-high-risk
- Possibility for voluntary application of other requirements (e.g. environmental and social sustainability)

New special rules for General Purpose AI models (GPAI)

GPAI models: trained on large data, can competently perform wide range of tasks and be integrated in numerous downstream applications; research, development, and prototyping activities preceding the placement on the market are not covered.

All GPAI
(lower tier)

- Information and documentation requirements, mainly to achieve **transparency for downstream providers**
- Policy to respect copyright and a summary of the content used for training purposes
- **Free and open-source models are exempted** from transparency requirements, when they do not carry systemic risks except from the copyright-related obligations

GPAI with systemic risks
(higher tier)

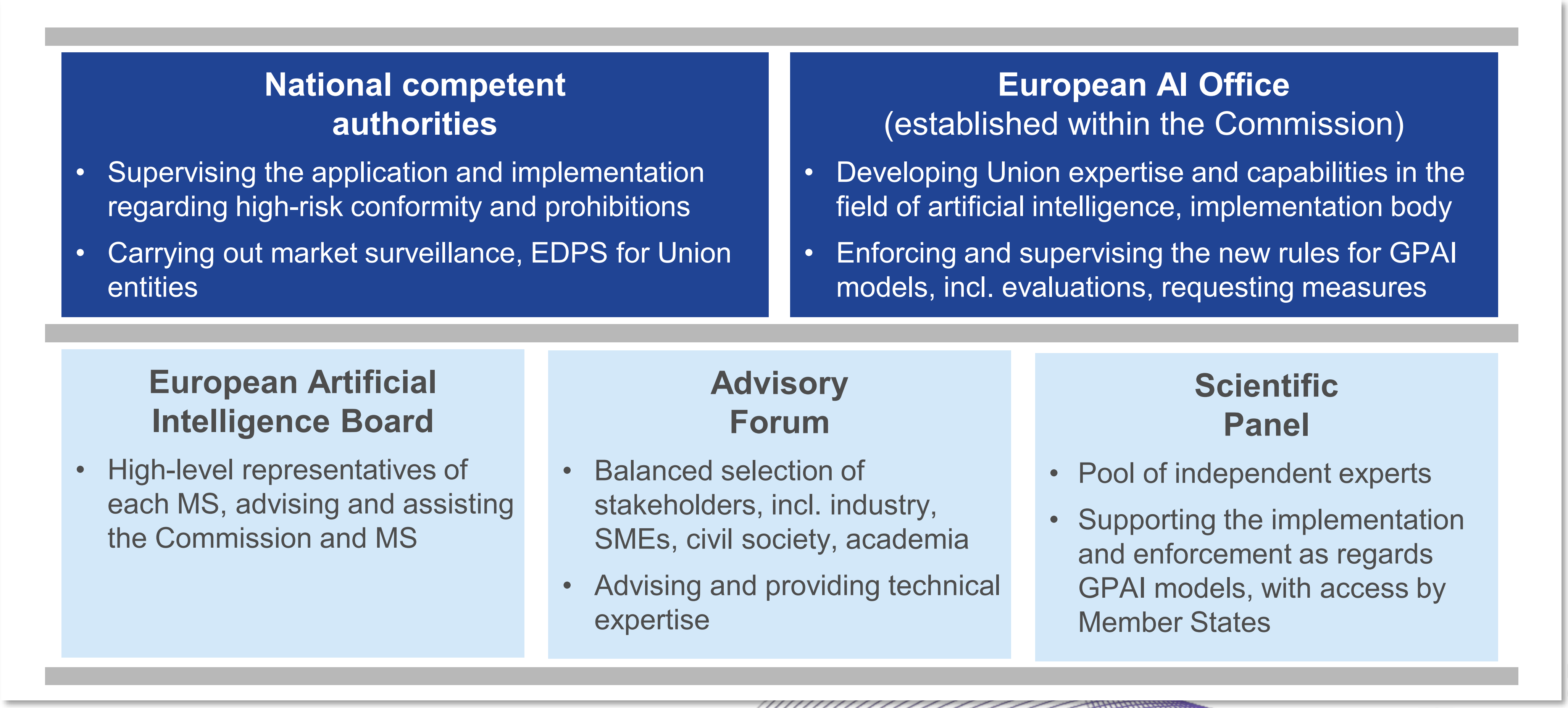
- **at least 10^25 FLOPs** or **designated by the AI Office** (e.g. based on benchmarks for capabilities, user count)
- All obligations from the lower tier **+ state-of-the-art model evaluations** (including red teaming / adversarial testing**), risk assessment and mitigation, incident reporting, cybersecurity and additional documentation**

updateable via delegated acts

- GPAI providers may rely on **Codes of Practice** to demonstrate compliance
- Codes of practice to be developed by industry under coordination of AI Office, the scientific community civil society and other experts also involved; the codes could be approved by COM through implementing act;
- New standardisation deliverable on GPAI to supersede the codes once EU harmonised standards available

A holistic governance structure for effective enforcement

Enforcement by national competent authorities and the AI Office
with a supportive structure for close collaboration with Member States and for additional technical expertise



National competent authorities

- Supervising the application and implementation regarding high-risk conformity and prohibitions
- Carrying out market surveillance, EDPS for Union entities

European AI Office
(established within the Commission)

- Developing Union expertise and capabilities in the field of artificial intelligence, implementation body
- Enforcing and supervising the new rules for GPAI models, incl. evaluations, requesting measures

European Artificial Intelligence Board

- High-level representatives of each MS, advising and assisting the Commission and MS

Advisory Forum

- Balanced selection of stakeholders, incl. industry, SMEs, civil society, academia
- Advising and providing technical expertise

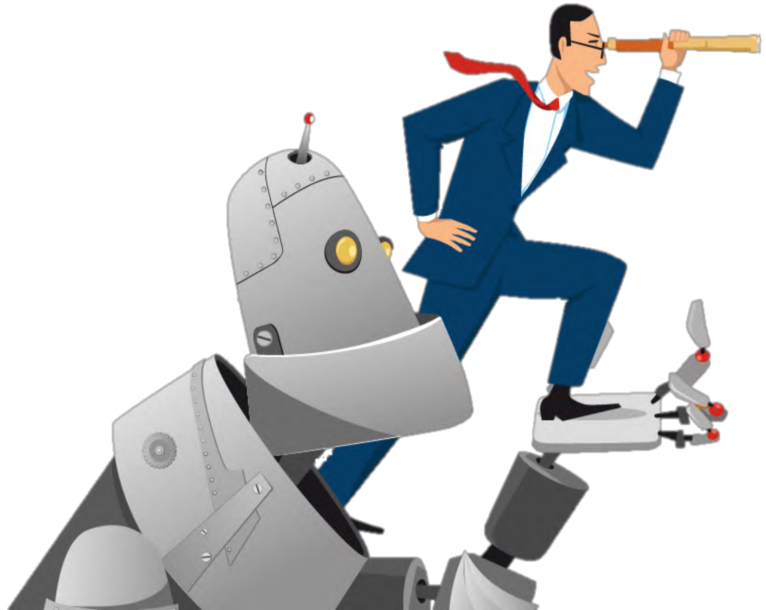
Scientific Panel

- Pool of independent experts
- Supporting the implementation and enforcement as regards GPAI models, with access by Member States

AI Office: Mission and tasks

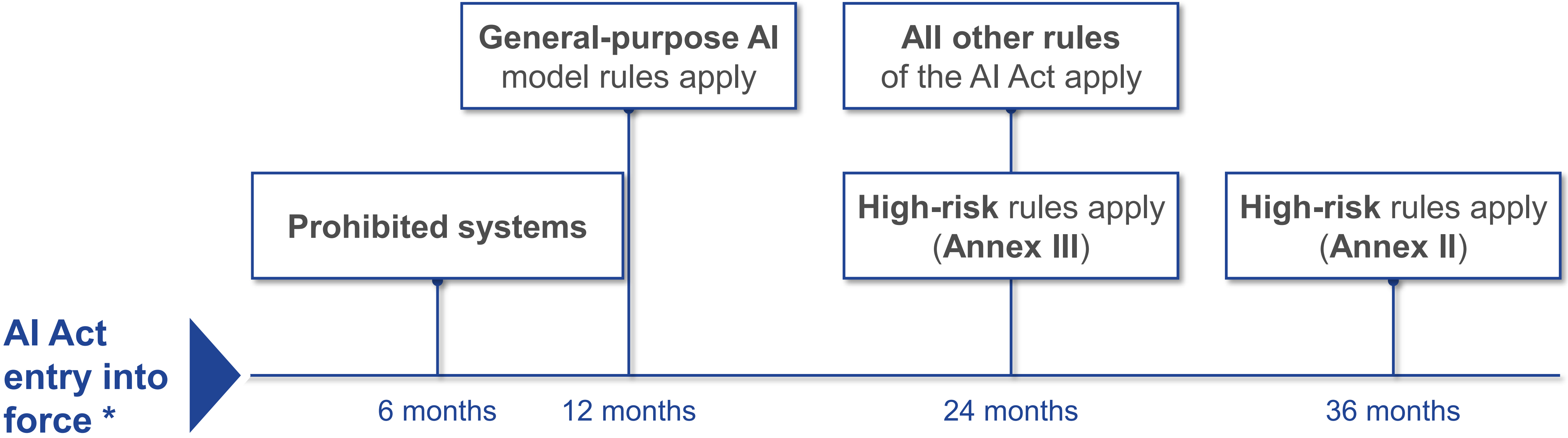
Context:

- ❖ Clear need for EU-level governance system for AI (SotEU 2023)
- ❖ Political agreement on AI Act from 8 December introduces role of AI Office
- ❖ Part of DG CNECT



- Responsibility to implement and enforce the AI Act, in particular rules on general-purpose AI models and systems
- Cooperate with all relevant EU bodies and Member States
- Collaboration with stakeholder community
- Cross-sectoral cooperation within the Commission
- Promote uptake of and innovation in AI with societal benefits
- Coordinate and promote international cooperation on AI

The AI Act enters into application in a gradual approach



AI Act entry into force *

6 months: **Prohibited systems**

12 months: **General-purpose AI** model rules apply

24 months: **All other rules** of the AI Act apply

24 months: **High-risk** rules apply (**Annex III**)

36 months: **High-risk** rules apply (**Annex II**)

*Following its adoption by the European Parliament and the Council, the AI Act shall enter into force on the twentieth day following that of its publication in the official Journal.

DIGITAL COMMISSION ESSENTIALS

European Commission

AI Act Implementation

European
Commission

Priority deliverables in the first 18 months

- First 6 months:
  - Commission implementing act revising the standardisation mandate
  - Commission implementing act on the establishment of a scientific panel of independent experts
  - Commission guidelines on the practical implementation of the AI system definition
  - Commission guidelines on practical implementation of prohibition, incl. reporting template for MSs for use of real-time remote biometric identification in publicly accessible spaces for law enforcement purposes

Priority deliverables in the first 18 months (Cont.)

- First 12 months:
  - Commission implementing act on modalities for evaluation of GPAI models
  - Commission guidance on reporting serious incidents
  - Report evaluating the need to update the list of high-risk use cases in Annex III and list of prohibited practices
  - Template for summary of content used to train GPAI model + assessment of codes of practice for GPAI models
  - Commission assessment of the code of practice developed by providers of GPAI models

Priority deliverables in the first 18 months (Cont.)

- First 18 months:
  - Commission guidelines on high-risk classification incl.:
    - high-risk filter for Annex III,
    - concepts of substantial modification and safety component &
    - application of high-risk requirements and obligations +
    - template for FRIA
  - Commission guidelines on transparency obligations
  - Commission implementing act on modalities for AI regulatory sandboxes
  - Commission implementing act on details for real-world testing plan

Research and Innovation in DG HOME

European Commission

Horizon Europe Cluster 3: Civil Security for Society

- A work programme structured in 6 destinations

FIGHTING CRIME AND TERRORISM

BORDER MANAGEMENT

RESILIENT INFRASTR.

DISASTER RESILIENT SOCIETIES

STRENGTHENED SECURITY R&I

CYBERSECURITY

Capability-based approach

End-User oriented

Societal dimension

Synergies and market creation

Relevant Horizon Europe projects in Border Management

- **Innovation for integrated information management and sharing:**
  - CLOSEYE, *Collaborative evaLuation Of border Surveillance technologies in maritime Environment bY pre-operational validation of innovativE solutions.*
  - AI-ARC, *AI-based, CISE-compatible virtual control room for maritime situational awareness.*
  - *NESTOR, Pre-frontier situational awareness beyond sea and land borders.*
  - EFFECTOR, *Interoperability, data fusion and analytics for maritime surveillance and cooperation between operating authorities and on-site intervention forces in real time, through a secure network.*
  - CISE-ALERT, *CISE's operationalization launch through a Long Endurance and Real live Test.*
  - PROMENADE, *ImPROved Maritime awarENess by means of AI and BD mEthods.*
  - SMAUG (Smart Maritime and Underwater Guardian). *Improve the underwater detection of threats in ports and their entrance routes*

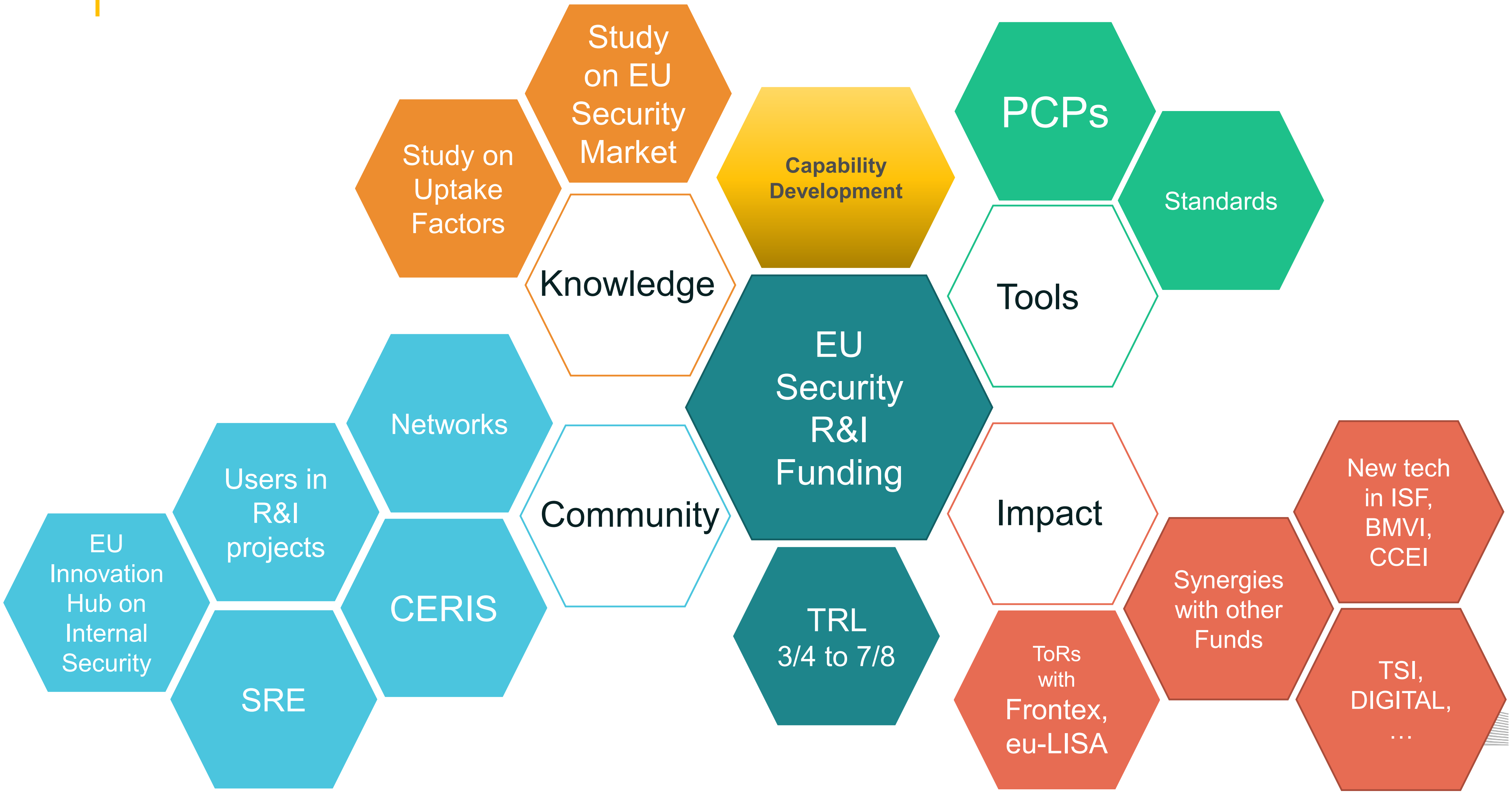
- **Innovative technologies for maritime situational awareness.**
  - ROBORDER, *Autonomous swarm of heterogeneous RObots for BORDER surveillance*
  - REACTION, *REal-time ArtifiCial InTellIgence for BOrders Surveillance via RPAS data aNalytics to support Law Enforcement Agencies.*
  - COMPASS2020, *Capabilities of unmanned technologies to support maritime patrol.*
  - *I-SEAMORE, High altitude platforms technology, satellite imagery, UxVs and ground-based sensors for maritime borders and situational awareness.*
  - *EURMARS, High altitude platforms technology for border surveillance.*

Relevant Horizon Europe projects in Border Management (continued)

Travel facilitation and flow of goods and passengers

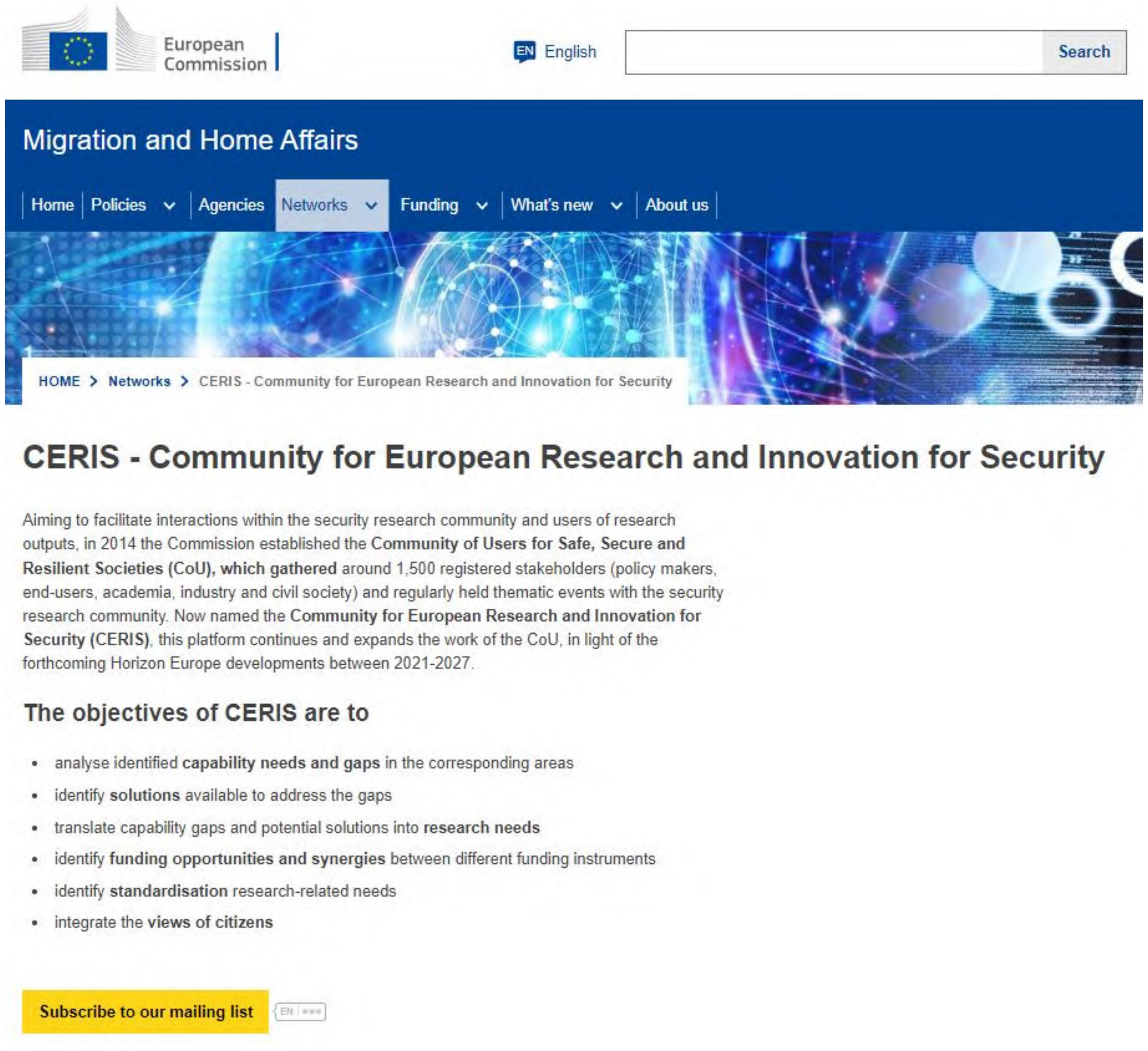
- ITFLOWS, *IT tools and methods for managing migration FLOWS*
- BAG-INTEL, *An intelligent system for improved efficiency and effectiveness of the customs control of passenger baggage from international flight arrivals.*
- METEOR, *Rapid, portable and reliable cargo screener - New concept of vapour screening technology - Ion Mobility Chemical Fingerprint Detector*
- BORDERSENS, *Border detection of illicit drugs and precursors by highly accurate electro sensors.*
- SILENTBORDER, *Cosmic Ray Tomograph for Identification of Hazardous and Illegal Goods hidden in Trucks and Sea Containers*
- COSMOPORT, *Using cosmic rays for better, more portable and efficient analysis and detection for customs*
- I-MARS, *image manipulation attack resolving solutions (documents fraud at borders)*

Addressing civil security innovation in the EU



European Commission

Community for Research and Innovation for Security (CERIS)

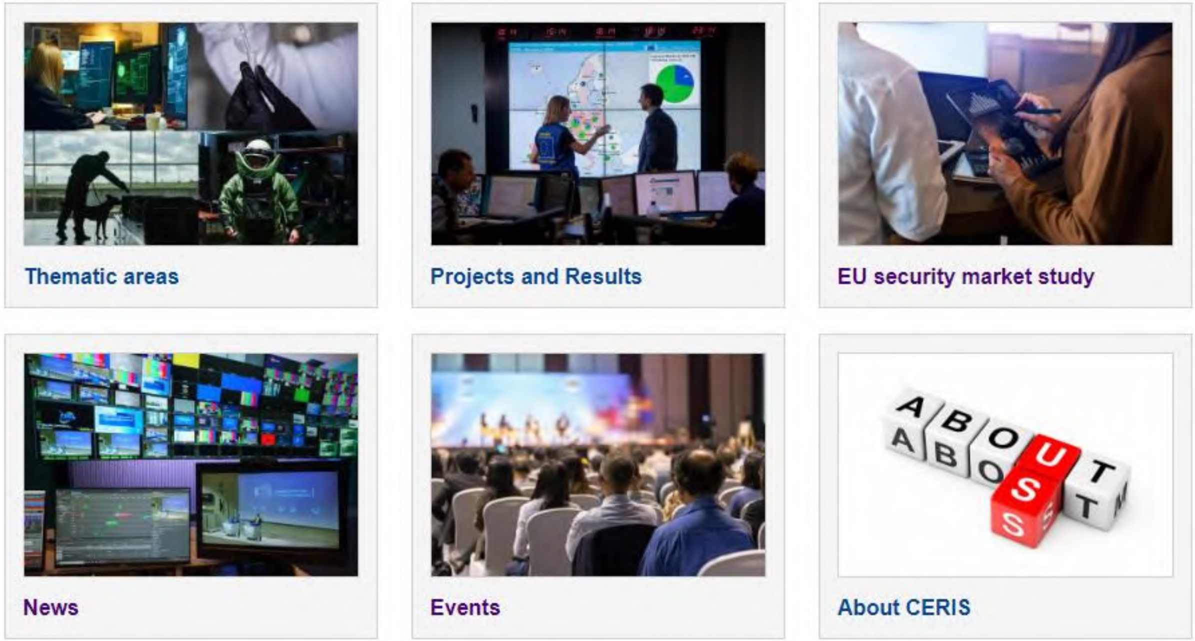

European Commission
EN English
Search
Migration and Home Affairs
Home
Policies
Agencies
Networks
Funding
What's new
About us
HOME > Networks > CERIS - Community for European Research and Innovation for Security

CERIS - Community for European Research and Innovation for Security

Aiming to facilitate interactions within the security research community and users of research outputs, in 2014 the Commission established the **Community of Users for Safe, Secure and Resilient Societies (CoU), which gathered** around 1,500 registered stakeholders (policy makers, end-users, academia, industry and civil society) and regularly held thematic events with the security research community. Now named the **Community for European Research and Innovation for Security (CERIS)**, this platform continues and expands the work of the CoU, in light of the forthcoming Horizon Europe developments between 2021-2027.

The objectives of CERIS are to

- analyse identified **capability needs and gaps** in the corresponding areas
- identify **solutions** available to address the gaps
- translate capability gaps and potential solutions into **research needs**
- identify **funding opportunities and synergies** between different funding instruments
- identify **standardisation** research-related needs
- integrate the **views of citizens**



Thank you

Slide xx: element concerned, source: e.g. Fotolia.com; Slide xx: element concerned, source: e.g. iStock.com

European Commission