EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

Strategic and operational threat analysis at Europol's EC3

Dr. Philipp Amann, MSc
Senior Strategic Analyst
Team Leader Strategy & Development

ENISA Workshop on EU Threat Landscape
24 February 2015

EC3 – Who We Are and What We Do

European Cybercrime Centre

EC3's History

2011-2012
RAND Feasibility Study for a European Cybercrime Centre

28 March 2012
Communication of the European Commission on the establishment of EC3

8 June 2012
European Council of Ministers endorsement

12 June 2012
First EC3 Programme Board

18 June 2012
EC3 Blueprint

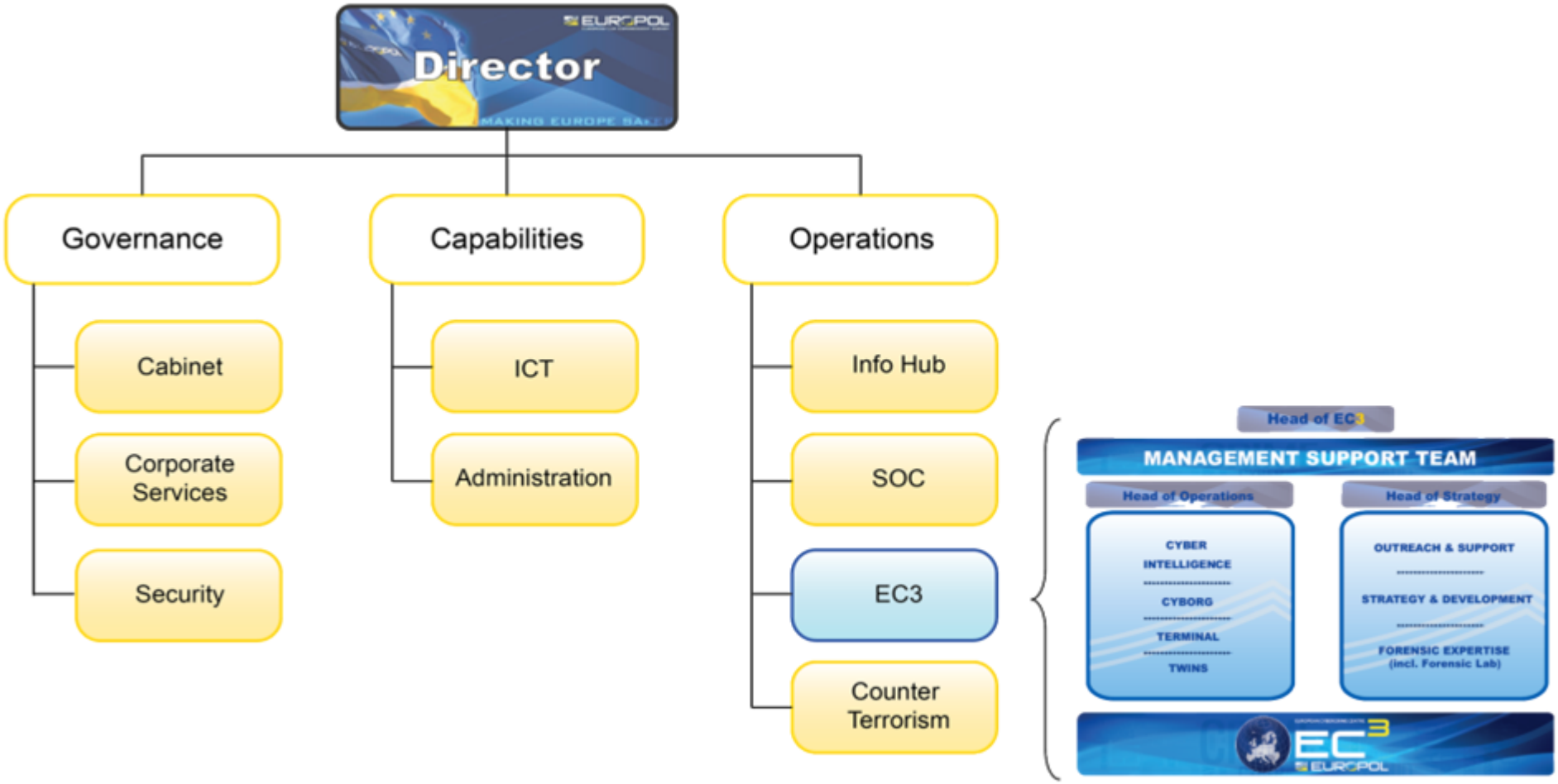
1 July 2012
EC3 Implementation Team starts its activities

23 October 2012
2nd EC3 Programme Board

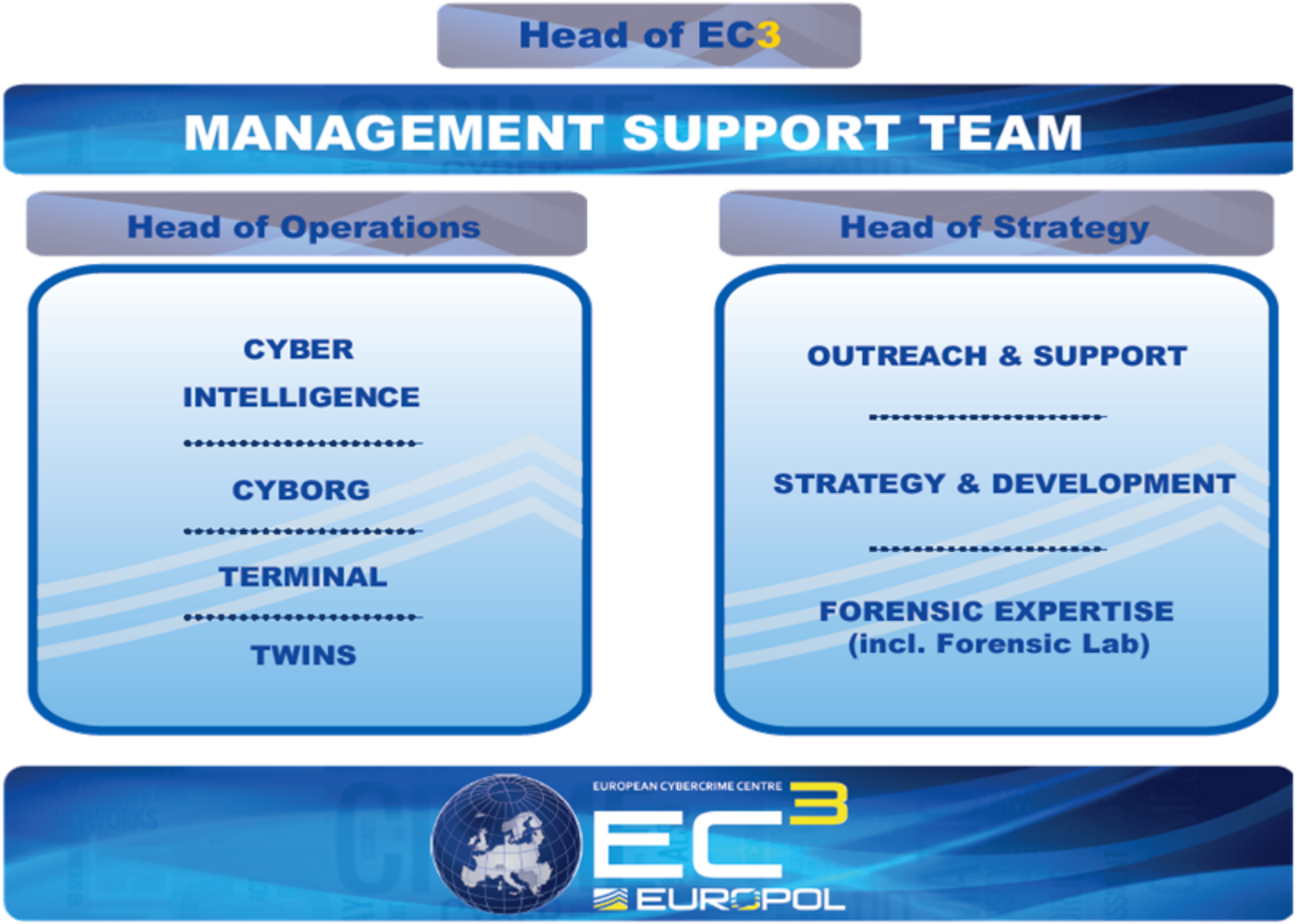
1 January 2013
EC3 is live

11 January 2013
EC3 Inauguration

Europol Organisational Structure



EC3 Organisational Structure



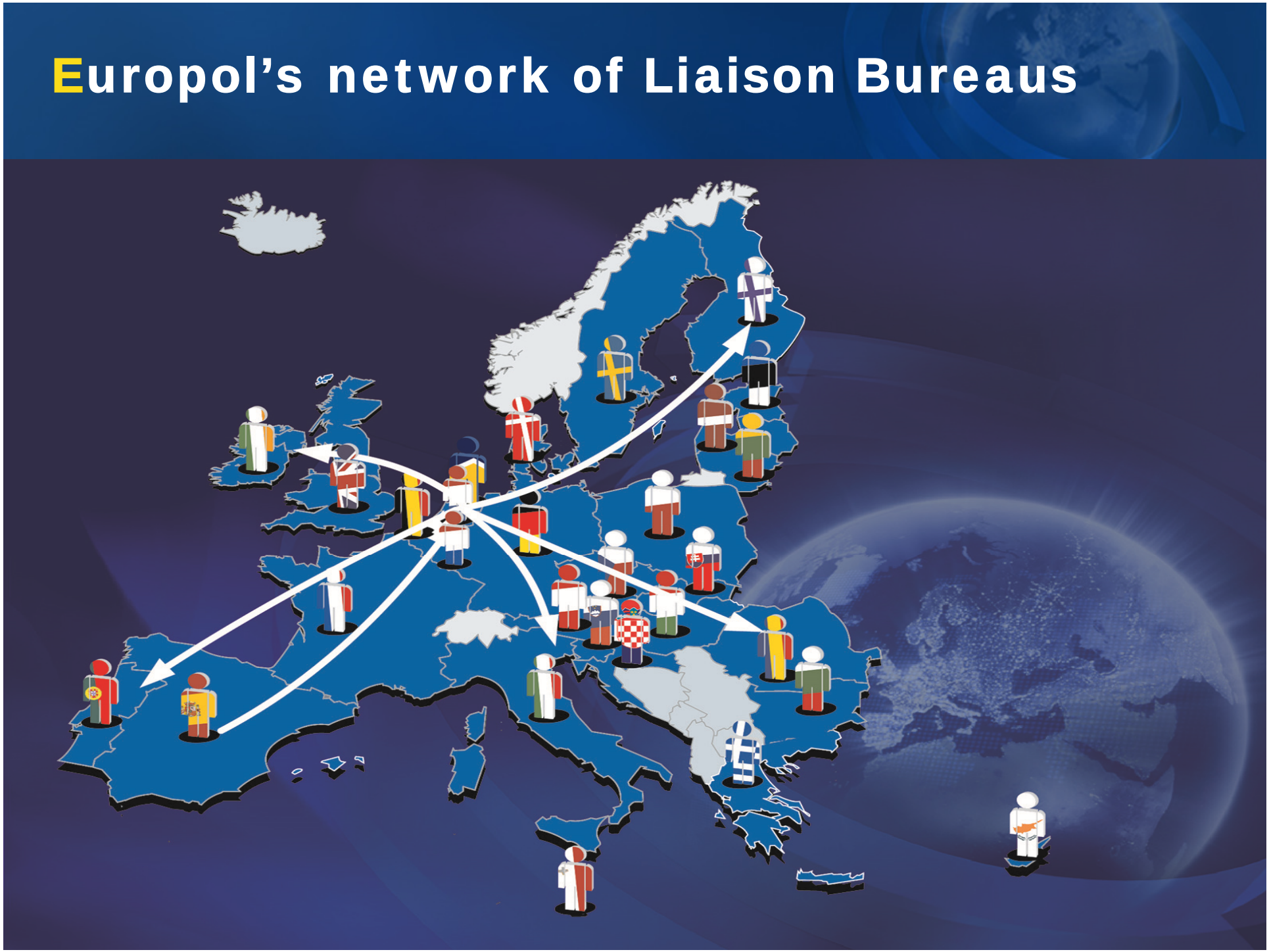
EC3 Governance Model

Assisted by 2 Advisory Groups

EUROPEAN CYBERCRIME CENTRE
EC3 EUROPOL

Multi-Stakeholder Approach

Europol's network of Liaison Bureaus



EC3 Core Services

European cybercrime info/intel focal point

Support to Member States' cybercrime investigations

Platform to pool skills and expertise & tool support for MS

Collective voice of European cybercrime investigators

OPERATIONAL

- Coordination of High Profile Operations
- On-the-Spot Operational Support
- Operational, Technical and Forensic Analysis
- Digital IT Forensics Support

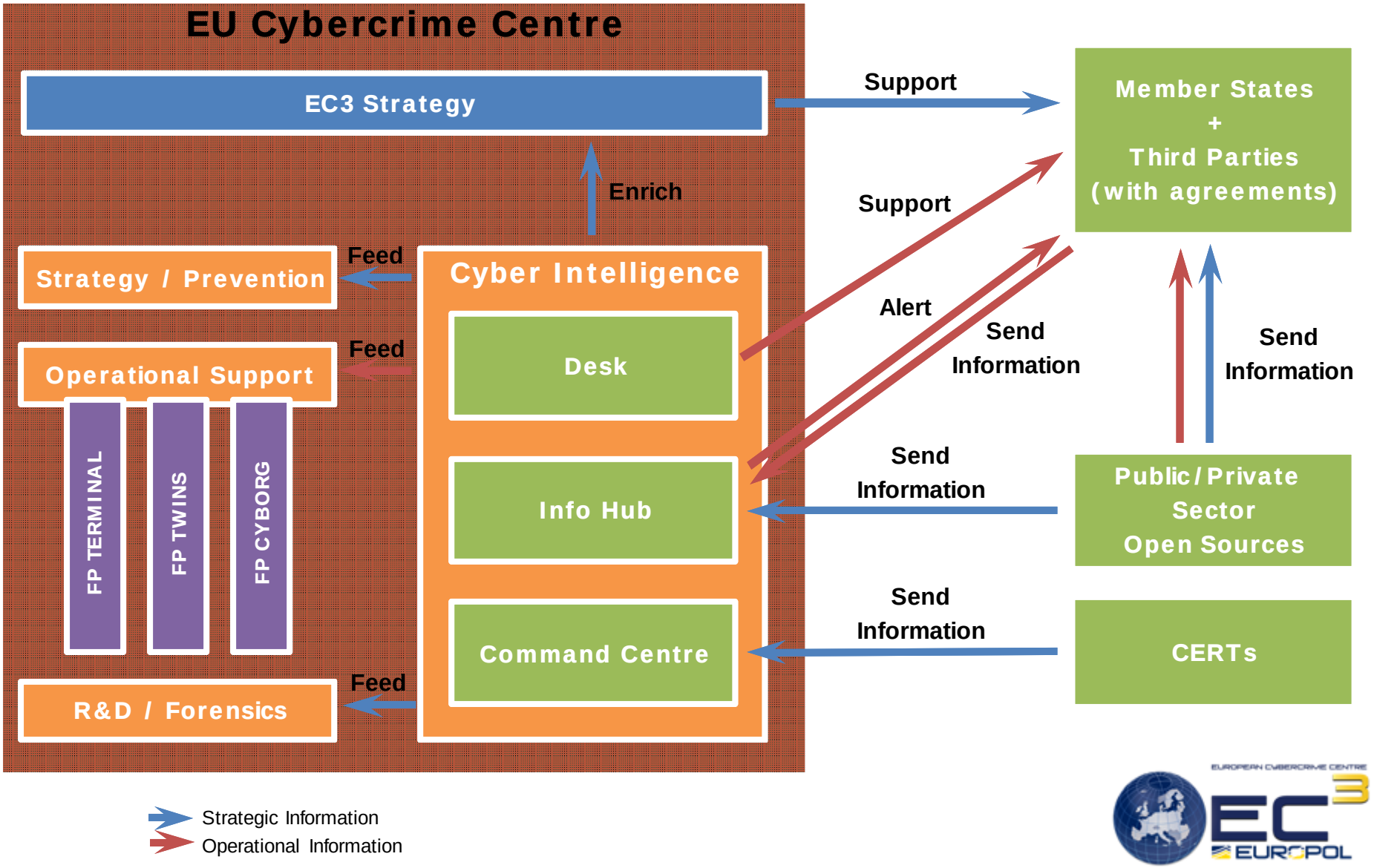
STRATEGIC

- Outreach to Public/Private Partners
- Strategy and Forward Looking Assessments
- Training and capacity building
- Digital IT Forensics R&D

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

EC3 Products & Solutions

EC3 Information / Intelligence Flow



Cyber Intelligence Team

Information collection on cybercrime from the widest array of public, private and open sources.

Analytical hub (tactical and operational), processing and analysing information from various sources.

Broaden information picture on cybercrime in Europe over time so as to rapidly identify emerging threats. **In close co-operation with Strategy.**

Pro-actively scans the environment, identifying new trends and patterns, updating stakeholders accordingly. **In close co-operation with Strategy.**

What Cyber-Intel can do

- OSINT
- Receive operational information from MS and operational partners
- Search Europol operational information

What Cyber-Intel cannot do

- Surveillance
- Engage with suspects
- Infiltration: provide opinions; create reputation
- "Control the crime" using agent provocateur

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

Strategy and Development Team

To provide Europol's EC3, EU law enforcement and other relevant partners, including EU policy makers, with an overview of trends, developments, capabilities and intentions to support the fight against cybercrime, inform the formulation of policies and legislative measures, contribute to the development of standardized training, awareness raising and preventive measures, and facilitate regular meetings of stakeholder and governance bodies.

EC3 Intelligence / Knowledge Products

CYBER-INTEL

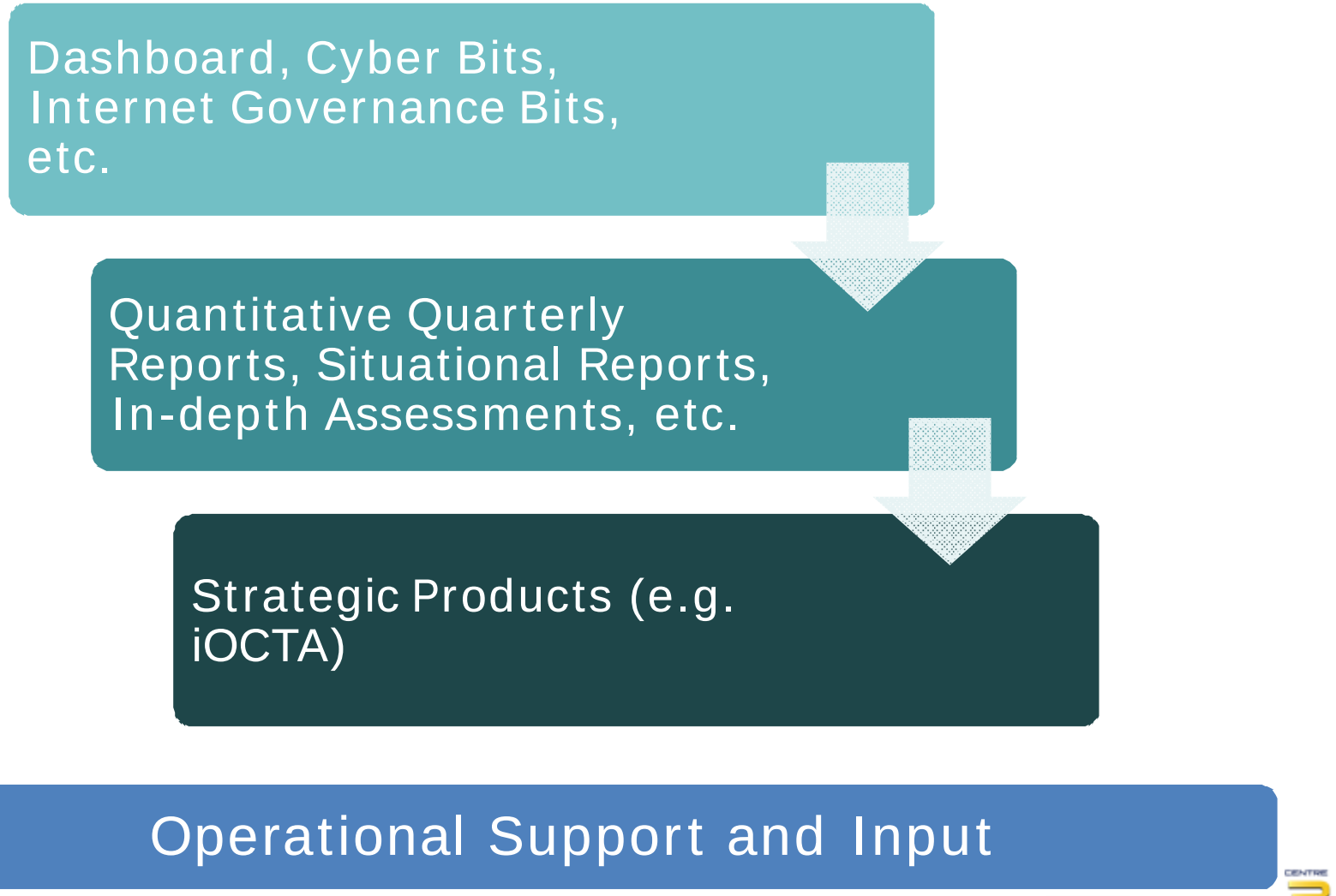
- **Cyber Bits**
  - **Trends**: Modus operandi, tool or technique used by cyber criminals. Emerging patterns and crime series.
  - **Knowledge**: Offer guidance and raise awareness.
  - **Technology**: Technical developments having impact law enforcement work.
  - **Tools:** Presentation of tailored tools to support operational activities.
- **OSINT Dashboard**
- **Quantitative Quarterly Report on Cyber Threats – in cooperation with Strategy**

STRATEGY

- **iOCTA**
- **Project 2020: Scenarios for the Future of Cybercrime**
- **Police Ransomware Threat Assessment**
- **A Review of Criminal Forums**
- **Strategic Assessment on CSE Online**
- **ICANN Guide for Dummies, Assessment of Bitcoin, Top 10 External Cyber Threats, etc.**

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

EC3 Intelligence / Knowledge Products



EC3 Threat Analysis – Some Definitions

- Data – value, word or event out of context i.e. without meaning.
- Information – data put into a meaningful context e.g. by using meta-data to provide context.
- Intelligence – 'actionable information' i.e. evaluated information that has strategic/operational/tactical value, particularly in the context of investigations.
- Evidence – information or intelligence that can be used in court.

EC3 Threat Analysis – Some Definitions

- Threat analysis – systematic detection, identification, and assessment of actual or potential cyber risks, the probability of these risks occurring and the consequences or impact should they occur.

EC3 Threat Analysis – Challenges

CYBER-INTEL

- Operational data vs. strategic data
- Sharing with non-competent authorities, particularly the private sector
- Sharing with non-operational partners
- Data retention
- Amount of data/information/intelligence
- Human resources, including language skills

STRATEGY

- Operational/tactical intelligence vs. Strategic threat intelligence - risk of separate intelligence cycles
- Forward-looking, more high-level decisions and planning support vs. Operational support
- Management support for Strategic Analysis
- Communication and analysis tasking and prioritisation process (e.g. selection of topics, Ops input)

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

EC3 Threat Analysis – Challenges

CYBER-INTEL & STRATEGY

- Access to data, information and intelligence (willingness to share, cost factor, lack of standards, overlapping data sets, lack of historical data, etc.)
- Limited OSINT capabilities, particularly in relation to Darknets
- Network of external partners, including industry and academia as well as other EU agencies and the CERT community
- Tool support (storage, retrieval, collation, correlation, analysis, visualisation, etc.)

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

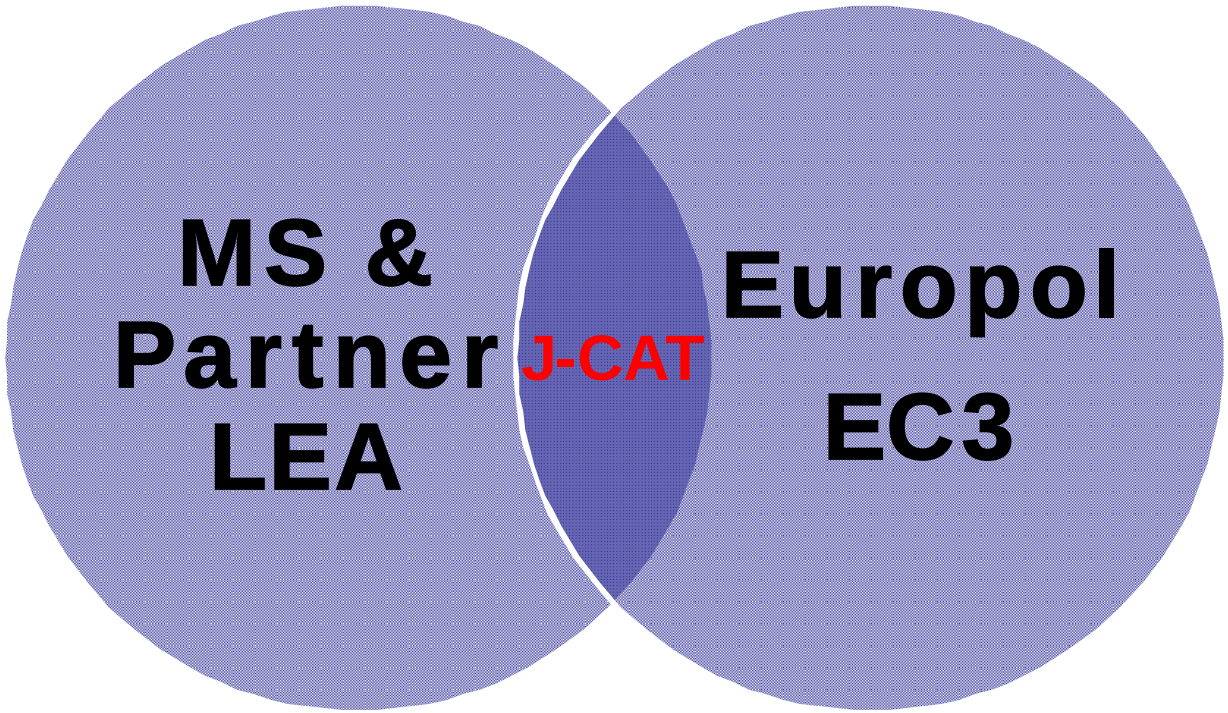
EC3 Threat Analysis – Initiatives

- Development of a taxonomy and business case for the exchange of information/intelligence between LE and CERTs
- Anonymized cross-matching solution
- Active Stakeholder Management and engagement with EU and non-EU partners, including with private industry and academia
- Engaged in internal and external discussions around OSINT capabilities and data protection

EC3 Threat Analysis – Initiatives

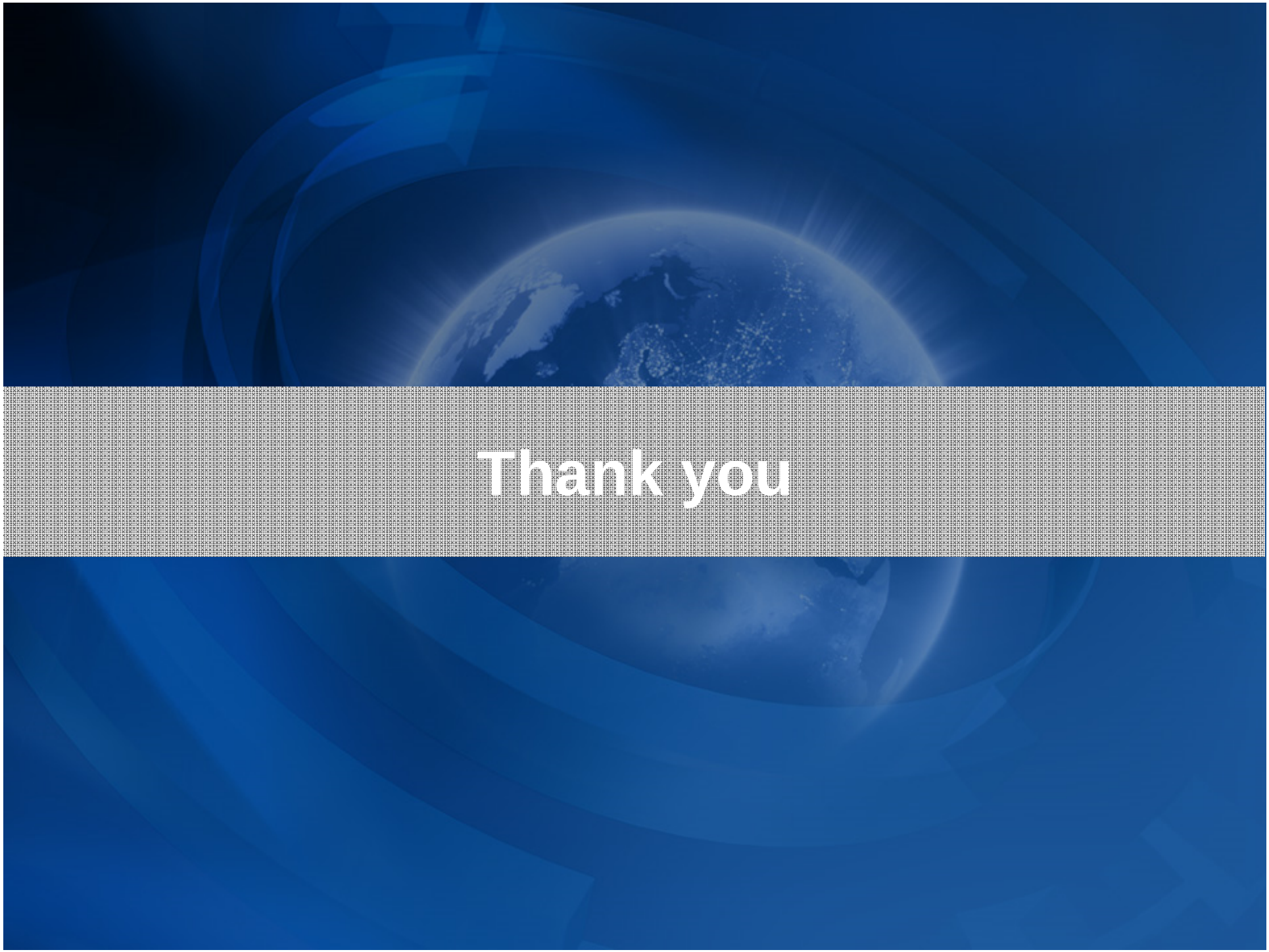
- In-house R&D
- Ongoing evaluation of commercial tools and services
- Training and capacity building
- ...

Joint Cybercrime Action Taskforce



EC3 Threat Analysis – Summary

- Two threat analysis areas– strategic and tactical/operational
- Privacy and data protection, and policies governing OSINT activities
- Exchange of data/information/intelligence with competent authorities vs. other partners
- Tool support and human resources


Thank you