Enhancing the Security of European Critical Information Infrastructures

ENISA's Activities

Dr. Evangelos OUZOUNIS
Head of Critical Information Infrastructure Protection & Resilience Unit
ENISA

ENISA

- Established in 2004
- **Centre of Excellence on cyber security** (e.g. cloud computing, exercises, national contingency plans)
- **Supporting the European Commission & Member States in their policy initiatives** (e.g. setting up and training CERTs, seminars for national exercises)
- **Facilitating cross-border cooperation** (e.g. supporting cyber security exercises)
- **Ensuring a coherent pan-European approach** (e.g. supporting the implementation of article 13a)

European Commission

Commissioner

Neelie **Kroes**

Vice-President
Digital Agenda

Cecilia **Malmström**

Home Affairs

Viviane **Reding**

Vice-President
Justice, Fundamental Rights and Citizenship

Maroš **Šefčovič**

Vice-President
Inter-Institutional Relations and Administration

Directorate-General

- Information Society and Media (DG CONNECT)
- Home (DG HOME)
- Justice(DG JUST)
- Human Resources and Security (DG HR)
- Informatics (DG DIGIT)

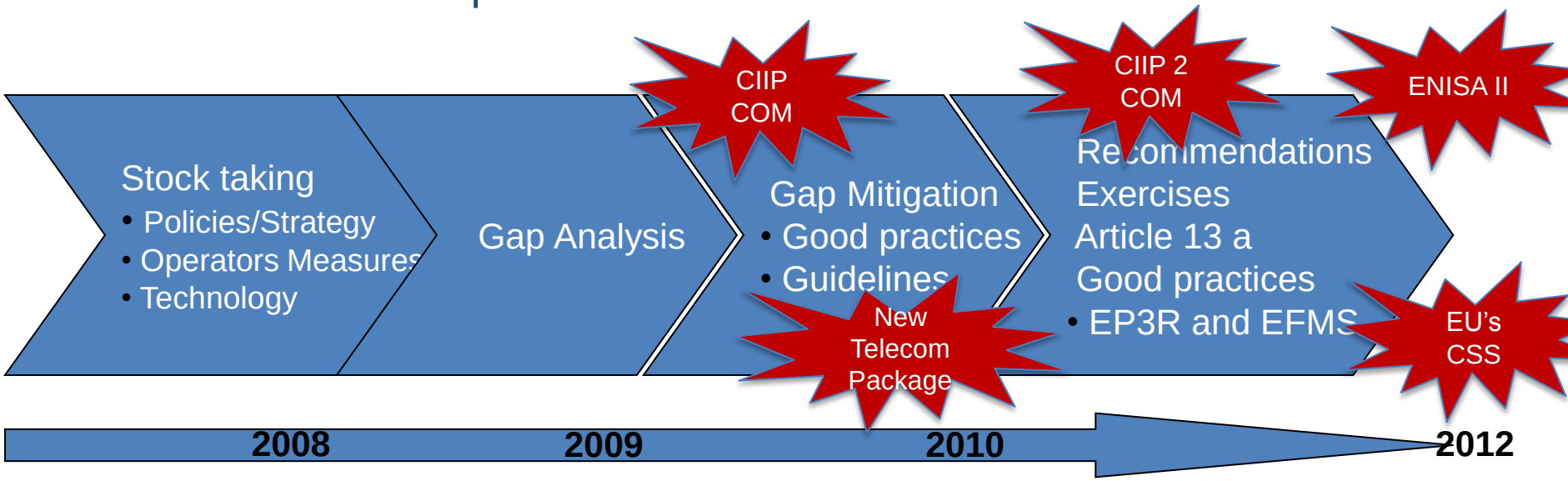
European Union Agencies

Agencies

- ENISA
- FRONTEX
- EUROPOL
- CEPOL
- EMCDDA
- EASO
- EUROJUST
- FRA (Fundamental Rights)

ENISA's Resilience and CIIP Unit

collectively improve European Critical Information Infrastructures and Resilience of European communications networks and services



EU Commission and at least 60% of the EU Member States made use of ENISA recommendations in their policy making process

Key EU Policy Milestones

- **CIIP Action Plan – COM Communication (2009)**
  - Pan European Public Private Partnership for Resilience (EP3R)
  - Pan European Forum for Member States (EFMS)
  - Exercises
- **Telecom Package – article 13 a (2009)**
  - Min. security requirements and guidelines for operators
  - Mandatory reporting of significant incidents to regulators
  - Annual reporting of incidents to ENISA and COM
- **Tallinn CIIP Ministerial Conference (2010)**
  - Cyber Europe 2010 – first pan European Exercise
- **ENISA II – new mandate (2010-2012)**
- **Balotonfured CIIP Ministerial Conference (2011)**
  - Cyber Atlantic 2011
- **CIIP 2 - COM Communication (2011)**
- **Internet/Cyber Security Strategy – (2012)**

Article 13 a – Mandatory Incident Reporting

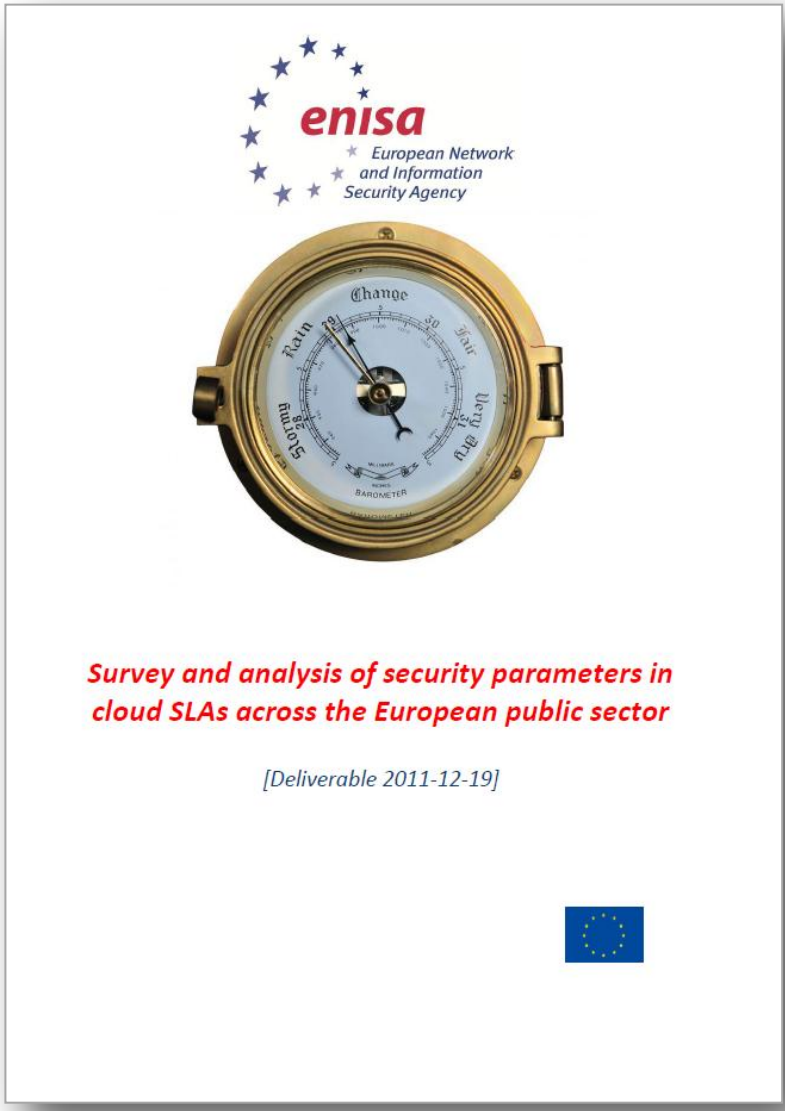
- facilitate a harmonised implementation of article 13 a across EU MS and providers
- provide support to individual NRAs
- propose appropriate technical measures to be considered by NRAs for deployment (bottom up, soft harmonisation)
- define the annual reporting scheme to ENISA & COM
- collect and analyse, on annual basis, national incident reports
- be informed on major, cross-country incidents

Cloud Computing

- Analyze Service Level Agreement (SLA).
- Propose solutions for continuous monitoring of SLAs
- Many customers do not monitor security measures continuously.
- Propose specific parameters and thresholds to monitor security
- Security parameters are less well covered.

Previous & Current Work

- 2009: Risk Analysis & Management
- 2009: Assurance Framework
- 2011: Security & Resilience of Gov Clouds
- 2012: Critical Clouds



Cyber Security Strategies & Insurance Policies

- Cyber Security Strategies (CSS)
  - stock taking of existing national cyber security strategies
  - engage experts via a thematic working group of key international experts
  - white paper with high level – level recommendations on CSS
  - validation of findings and finalisation of good practice guide
  - contribute to COM's Cyber Security Strategies

- Challenges and Incentives to Cyber Insurance
  - analyze the status of cyber insurances in EU and in the world
  - identify barriers and challenges that prohibit the development of insurances
  - validate the findings via a thematic expert group
  - provide recommendations to key stakeholders

EP3R
Public Private Partnership for Resilience

- provide a platform for information sharing and stock taking of good policy and industrial practices
- discuss public policy priorities, objectives & measures
- improve coherence and coordination of policies for security and resilience in Europe;
- 3 Working Groups
  - WG 1: Interdependencies of ICTs to critical Sectors
  - WG 2: Baseline requirements for security and resilience of electronic communication networks
  - WG 3: Coordination and cooperation mechanisms
    - Botnets
    - Pan European exercise

ICS – SCADA & Smart Grids

- ICS – SCADA study with key recommendations for stakeholders
- Smart Grids Study – High Level Recommendations
- Smart Grids Analysis on Min Security Measures
- Certification of Smart Grids Components
- Contribution to numerous initiatives
  - CEN/CENELEC standardization
  - Eurosscsie
  - ERNCIP
  - DG ENER and DG CONNECT initiatives
  - EU US working group

Cyber Crisis Co-operation

- Cyber Exercises
  - Cyber Europe 2010
  - Cyber Atlantic 2011
  - 2 regional cyber exercises (2012)
  - Cyber Europe 2012 (in planning)
  - roadmap for EU CIIP exercises
  - good practice guide
  - seminars to MS on national exercises
  - stock taking of national cyber exercises
  - scenarios for future CIIP exercises

- National Contingency Plans
  - good practice guide
  - seminars to MS on national contingency planning
  - contribute to the EU discussion on crisis co-operation framework(s)

Conclusions

- security & resilience of CII extremely important
- uneven and uncoordinated national & European activities
- European and international efforts to build procedures for responding to cyber crisis
- testing of such procedures via national, regional and European exercises is key!
- ENISA remains strongly committed to support EU MS and the Commission in addressing these challenges

Other Areas - Botnets

- **Open issues**
  - wide deployment of botnets in almost all cyber incidents
  - increased sophistication, easy access to tools
  - no real picture from statistics
  - socio-economic barriers in fighting botntes
  - lack of co-operation among key stakeholders
  - lack of support for bot victims (e.g. citizens, SMEs, ..)

- **Recommendations**
  - stimulate the commitment of stakeholders to work on the eradication of botnets (e.g via PPPs, e.g. EP3R)
  - MS and COM to provide a comprehensive policy framework (e.g. appropriate incentives, supportive legislation and suitable technical means) for ISPs, end-users, researchers and software producers to be able to implement effective defensive measures
  - support R&D on new emerging bot techniques
  - develop harmonised EU legislative measures to cyber crime
  - aware citizens and SMEs on the importance of botnets

Other Areas - Internet Interconnection Ecosystem

- **Open issues**
  - complex interconnected networks
  - no central Network Operation Centre for internet
  - little information about the size and shape of the Internet infrastructure or its daily operation
  - lack of transparency on interconnection and peering agreements
  - systemic cascading effects due to interdependences among providers

- **Recommendations - further work**
  - understand failures better – learn from past incidents,
  - develop active information sharing mechanisms on emerging threats and vulnerabilities
  - R&D on inter-domain routing, traffic engineering, redirection and prioritisation during a crisis
  - identify and promote good practices, engage stakeholders in the deployment of them through PPPs
  - greater transparency on how ISPs interconnect