EU policy on Network and Information Security & Critical Information Infrastructures Protection

Köln, 10 March 2011

Valérie ANDRIANAVALY
European Commission
Directorate General
Information Society and Media - DG INFSO
Unit A3 – Internet Governance; Network and Information Security
valerie.andrianavaly@ec.europa.eu

European Commission
Information Society and Media

EU Policy on NIS and CIIP

Agenda

1. **Digital Agenda for Europe**

2. **CIIP Action Plan**

3. **The European Public-Private Partnership for Resilience – EP3R**

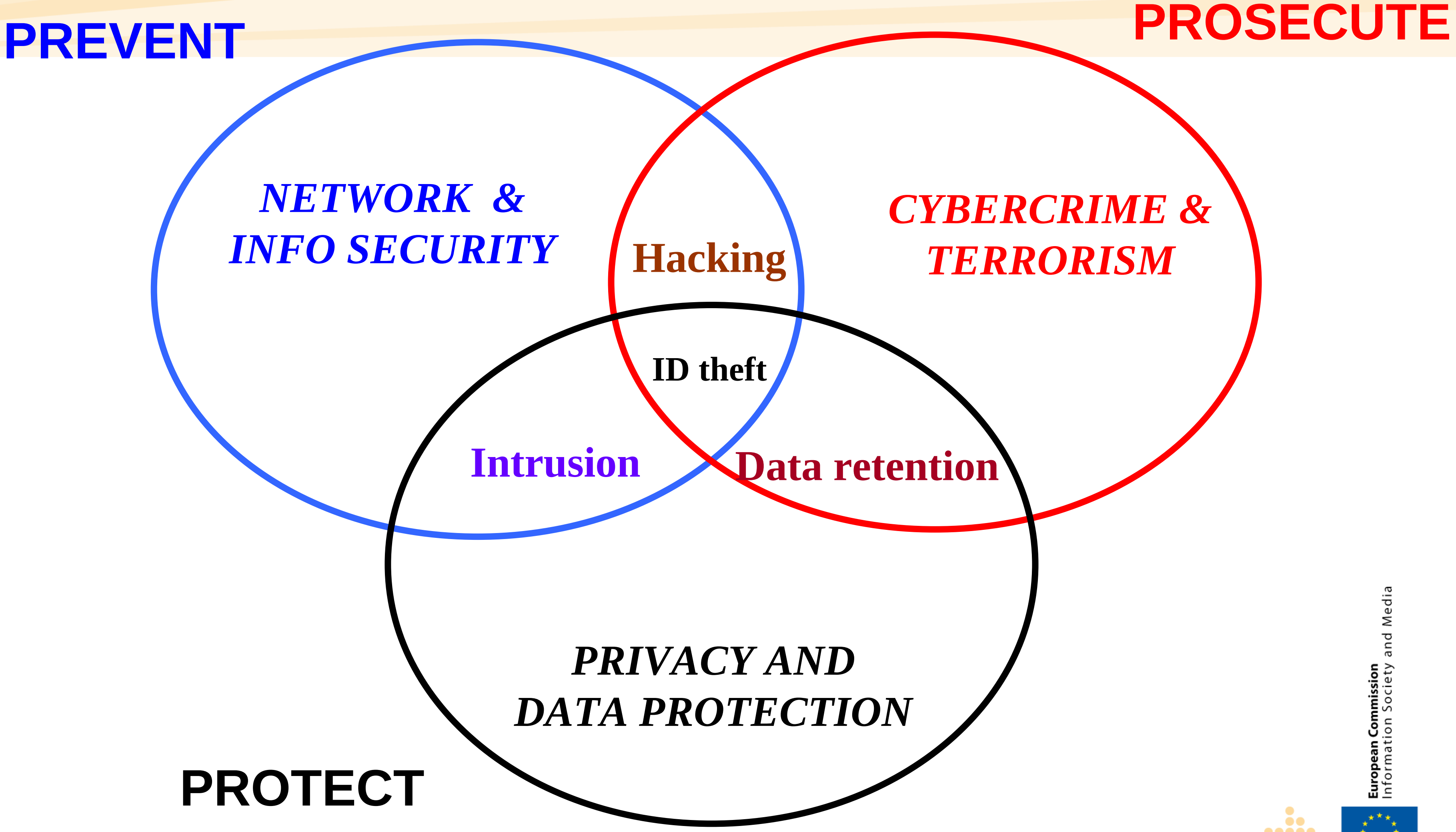
A Digital Agenda for Europe - COM(2010)245

The Seven Priority areas for action -

"Every European Digital"
N. Kroes – May 2010

1. **Creating a Digital Single Market**
2. **Improving the framework conditions for interoperability between ICT products and services**
3. **Boosting Internet trust and security**
4. **Guaranteeing the provision of much faster internet access**
5. **Encouraging investment in research and development**
6. **Enhancing digital literacy, skills and inclusion**
7. **Applying ICT to address social challenges such as climate change, rising healthcare costs and the ageing population.**

Three angles for actions on NIS Policy



PREVENT

PROSECUTE

NETWORK & INFO SECURITY

CYBERCRIME & TERRORISM

Hacking

ID theft

Intrusion

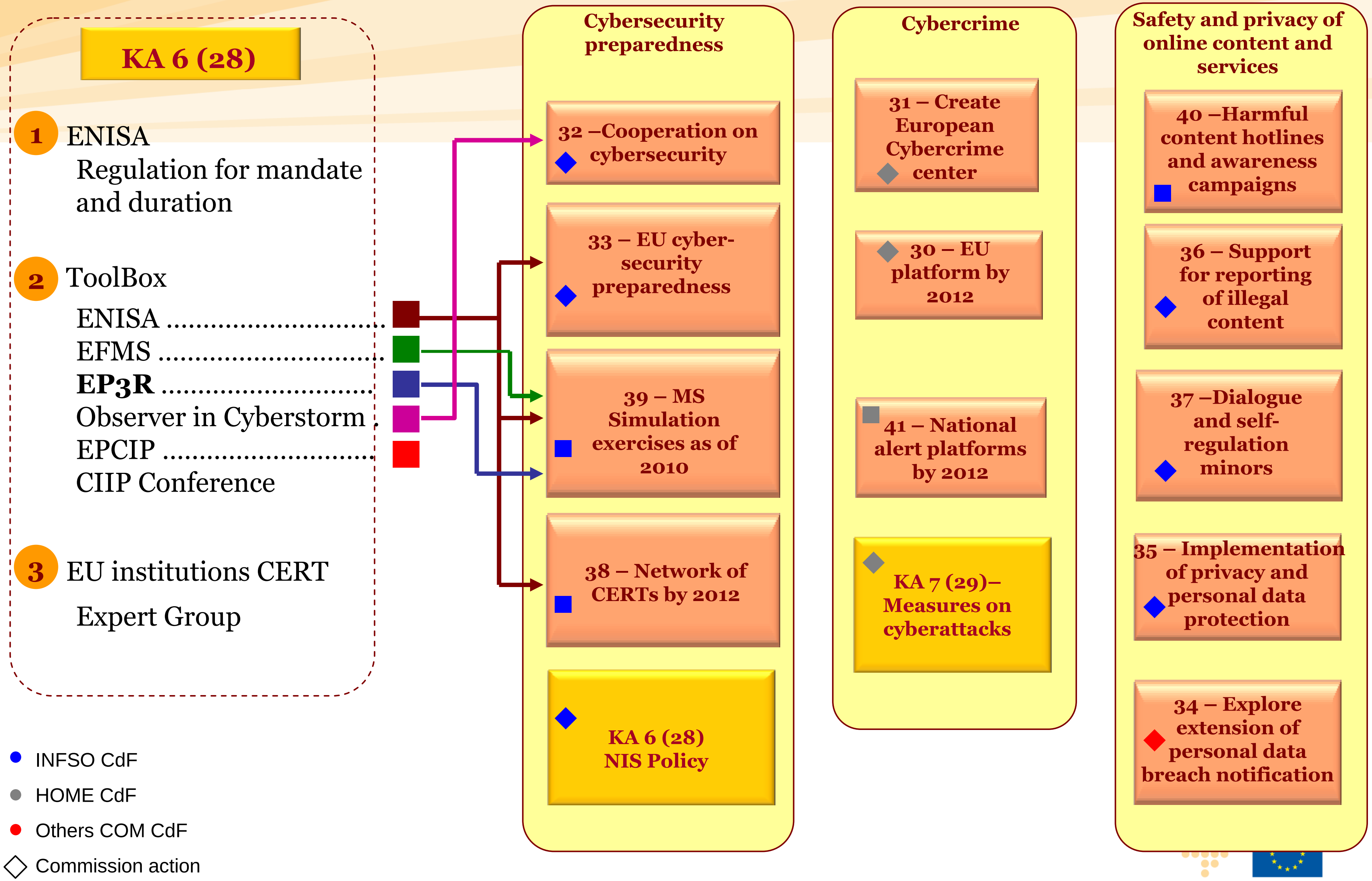
Data retention

PRIVACY AND DATA PROTECTION

PROTECT

European Commission
Information Society and Media

Overview of Pillar 3 "Trust and Security"



KA 6 (28)

1 ENISA
Regulation for mandate and duration

2 ToolBox
ENISA ……………………… ■
EFMS ……………………… ■
EP3R ……………………… ■
Observer in Cyberstorm . ■
EPCIP ……………………… ■
CIIP Conference

3 EU institutions CERT
Expert Group

Cybersecurity preparedness

- ◆ 32 –Cooperation on cybersecurity
- ◆ 33 – EU cyber-security preparedness
- ■ 39 – MS Simulation exercises as of 2010
- ■ 38 – Network of CERTs by 2012
- ◆ KA 6 (28) NIS Policy

Cybercrime

- ◆ 31 – Create European Cybercrime center
- ◆ 30 – EU platform by 2012
- ■ 41 – National alert platforms by 2012
- ◆ KA 7 (29)– Measures on cyberattacks

Safety and privacy of online content and services

- ■ 40 –Harmful content hotlines and awareness campaigns
- ◆ 36 – Support for reporting of illegal content
- ◆ 37 –Dialogue and self-regulation minors
- ◆ 35 – Implementation of privacy and personal data protection
- ◆ 34 – Explore extension of personal data breach notification

● INFSO CdF

● HOME CdF

● Others COM CdF

◇ Commission action

□ Member States action

Most recent policy developments

- **30 September 2010: Adoption by the Commission of two complementary proposals:**
  - **Proposal for a Regulation concerning ENISA (COM(2010)521)**
  - **Proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA - COM(2010)517**
- **20 November 2010: Establishment of the EU-U.S. Working Group on Cybersecurity and Cybercrime – EU-U.S. Summit – Lisbon**
- **22 November 2010: Adoption of EU Internal Security Strategy**
- **Forthcoming: Policy statement on CIIP achievements and next steps**

The proposal to modernise ENISA *COM(2010) 521 final*

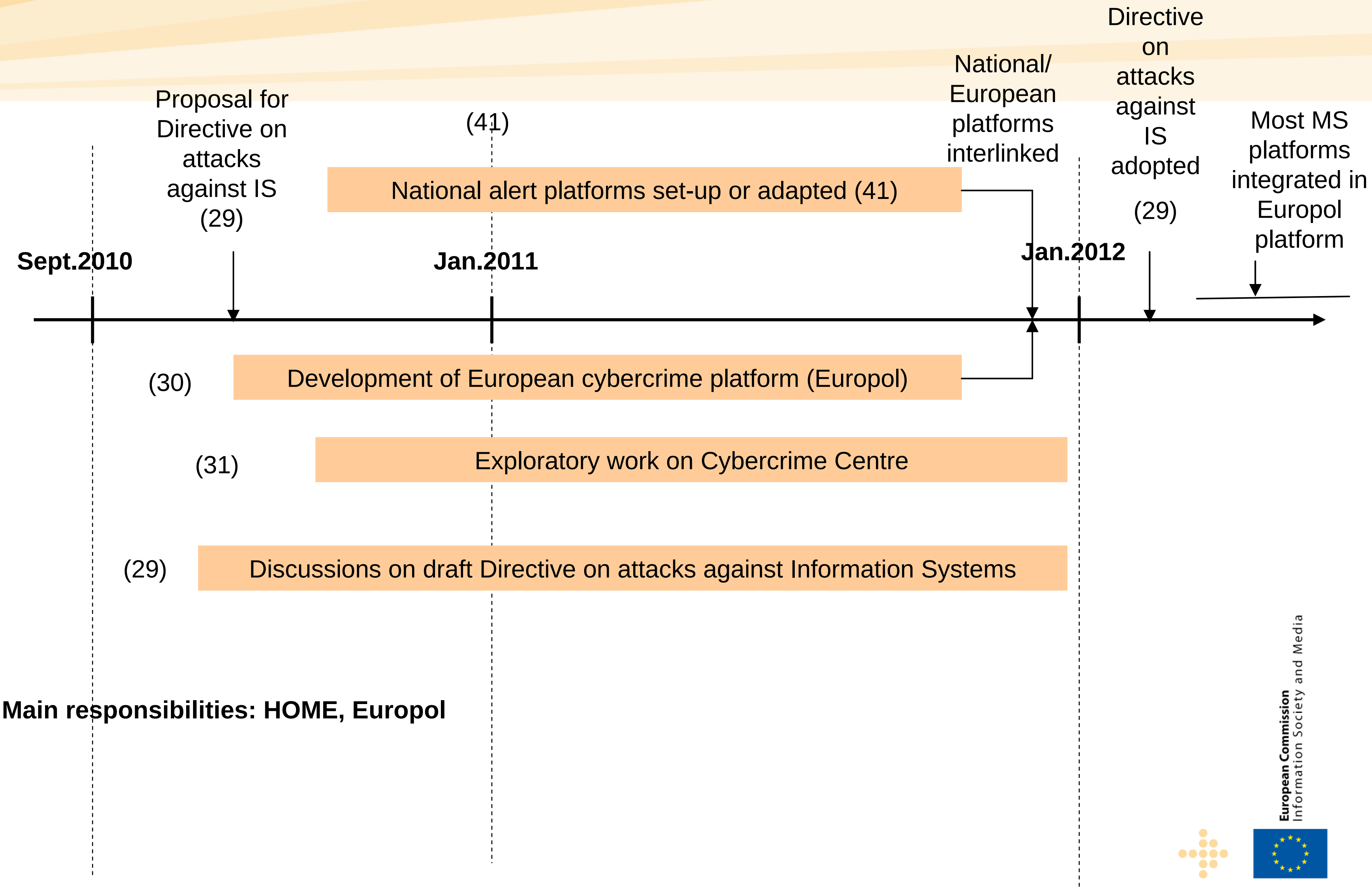
- 30 September 2010:
  - ➢ **Adoption by the Commission of its proposal for a Regulation concerning ENISA**
- Main objectives of the proposal:
  - ➢ **To reinforce and modernise the mandate of ENISA**
  - ➢ **To extend it with five years**
- Option 3 is the preferred policy option among the five options considered in the impact assessment

  => Expansion of functions currently defined for ENISA and adding law enforcement and privacy protection agencies as fully fledged stakeholders
- Proposal based on Art. 114 TFUE

The proposal to modernise ENISA COM(2010) 521 final *Role of the Agency*

- ENISA has two main roles
  - Give support, advice and expertise to the EU institutions and the Member States on all relevant aspects of the NIS policy
  - Facilitate the exchange of best practices and the cooperation between the actors of the sector (EU institutions, Member States, public bodies, private actors) in addressing NIS issues
- Proposed tasks attributed to ENISA will help the Agency fulfilling its role

Cybercrime



Proposal for Directive on attacks against IS (29)

(41)

National alert platforms set-up or adapted (41)

National/ European platforms interlinked

Directive on attacks against IS adopted (29)

Most MS platforms integrated in Europol platform

Sept.2010

Jan.2011

Jan.2012

(30) Development of European cybercrime platform (Europol)

(31) Exploratory work on Cybercrime Centre

(29) Discussions on draft Directive on attacks against Information Systems

Main responsibilities: HOME, Europol

The EU Internal Security Strategy in Action: Five steps towards a more secure Europe *COM(2010) 673 – 22 November 2010*

Objective 3: Raise levels of security for citizens and businesses in cyberspace

- **Action 2 - Work with industry to empower and protect citizens:**
  - **Cooperation bw public and private sector** must be strengthened on a European level through **EP3R**
  - EP3R should also **engage with international partners** to strengthen the global risk management of IT networks
- ***Action 3*** **- Improve capability for dealing with cyber attacks:**
  - Every MS, and the EU institutions should have a **well-functioning CERT by 2012**
  - MS should **network together their nat/gov CERTs** by 2012
  - Develop, with the support of EC and ENISA, **EISAS**, by 2013
  - MS to **develop national contingency plans**
  - MS to undertake regular national and European **exercises**

EU Policy on NIS and CIIP

Agenda

1. **Digital Agenda for Europe**
2. **CIIP Action Plan**
3. **The European Public-Private Partnership for Resilience – EP3R**

Communication on CIIP - COM(2009)149
Objectives and scope

- **High level objectives**
  - Protect Europe from large scale cyber attacks and disruptions
  - Promote security and resilience culture (*first line of defence*) & strategy
  - Tackle cyber attacks & disruptions from a systemic perspective

- **Means**
  - Enhance the CIIP preparedness and response capability in EU
  - Promote the adoption of adequate and consistent levels of preventive, detection, emergency and recovery measures
  - Foster International cooperation, in particular on Internet stability and resilience

- **Approach**
  - Build on national and private sector initiatives
  - Engage public and private sectors
  - Adopt an all-hazards approach
  - Be multilateral, open and all inclusive

Communication on CIIP COM(2009)149

Five specific objectives

1. Foster cooperation and exchange between MS
2. Develop a European public-private partnership
3. Enhance incident response capability
4. Promote the organisation of national and European exercises
5. Reinforce international cooperation

CIIP Policy - COM(2009)149

The Five Pillars of the CIIP Action Plan

1. **Preparedness and prevention**
   - **European Forum for MS** to share information & policy practices - EFMS
   - **European Public Private Partnership for Resilience EP3R**
   - **Baseline of capabilities and services** for National/Governmental CERTs

2. **Detection and response**
   - Development of a **European Information Sharing and Alert System** – EISAS dedicated to EU citizens and SMEs

3. **Mitigation and recovery**
   - National contingency planning and **exercises**
   - **Pan-European exercises** on large-scale network security incidents
   - Reinforced **cooperation between National/Governmental CERTs**

4. **International Cooperation**
   - Define European **priorities, principles and guidelines** for the long term **resilience and stability of the Internet**
   - Promote the principles and guidelines at global level
   - **Global cooperation on exercises** on large-scale Internet incidents

5. **Definition of criteria for the identification of European Critical Infrastructures in the ICT sector**

The CIIP Action plan

State of Play of the Implementation

- **EFMS:**
  - **European principles for the long term resilience and stability of the Internet**
  - **Criteria to identify ECIs in ICT sector**
  - **Long term strategy on pan-European exercises**
- **EP3R**
  - **Objectives, principles, structure and 3 WGs in Nov 2010:**
    1. **Key assets/ resources/ functions for e-communications**
    2. **Baseline requirements for security and resilience**
    3. **Cooperation to prevent and respond to large scale disruptions**
- **1st Pan-European exercises** on large-scale network security incidents organised on **4th of November 2010**
- Cooperation between **National/Governmental CERTs**
  - **Baseline of capabilities and services - ENISA Dec 2010**
- **EISAS:** Prototyping projects FISHA and NEISAS -> Q1 2011
- **International** Cooperation
  - **EU-U.S. Working Group & G8**

EU Policy on NIS and CIIP

Agenda

1. **Digital Agenda for Europe**

2. **CIIP Action Plan**

3. **The European Public-Private Partnership for Resilience – EP3R**

European Public-Private Partnership for Resilience – EP3R

Objectives and scope

Objectives:

- Information **sharing** and stock taking of good policy and industrial practices
- Foster a **common understanding** on the economic and market dimensions of security and resilience
- Discuss public policy **priorities**, **objectives** and **measures** to improve the coherence and **coordination** of policies for security and resilience in Europe.
- Identify and promote the adoption of **good baseline practices** and coordinated risk assessment approaches.

Scope:

- Focuses on **prevention and preparedness**
- With **European dimension** and in view of **global outreach**

European Public Private Partnership for Resilience (EP3R)

Key principles

- **Complementarity:** EP3R should **build upon and complement** existing national initiatives, benefit from ENISA's work and fully respect national responsibility, without duplicating efforts.
- **Trust:** EP3R should provide the structure, processes and environment for "**trusted collaboration**", including the protection of sensitive information.
- **Value**: set emphasis on **bi-directional exchanges** between public and private participants. EP3R should aim to deliver **concrete results**.
- **Competition:** Activities have to ensure that **market mechanisms** will not be distorted and **no elements or perception of cartel behaviour** would emerge. On the other hand, participation of competitors in EP3R should **not hinder the exchange** of information and good practices.
- **Openness**: EP3R should be open to **all stakeholders** which bear a part of the shared responsibility for resilience of CIIs.
- **Flexibility**: EP3R should be capable to **consider and adapt to evolving challenges and policy developments**.

EP3R – Working Groups
Areas of action

- **WG 1**: **Key assets/ resources/ functions** for the continuous and secure provisioning of electronic communications across countries

- **WG 2**: **Baseline requirements** for security and resilience of electronic communications

- **WG 3**: **Coordination and cooperation** needs and mechanisms to prevent and respond to large scale disruptions affecting electronic communications

➢Foster cooperation between relevant public-private partners towards the development of **European collaboration to fight botnets**.

EU Policy on NIS and CIIP

Thanks!

Web Sites

- **A Digital Agenda for Europe**
  http://ec.europa.eu/information_society/digital-agenda/index_en.htm

- **Commission to boost Europe's defences against cyber-attacks**
  http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=6190

- **EU policy on promoting a secure Information Society**
  http://ec.europa.eu/information_society/policy/nis/index_en.htm

- **EU policy on Critical Information Infrastructure Protection – CIIP**
  http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

- **The reformed Telecom Regulatory Framework - November 2009**
  http://ec.europa.eu/information_society/policy/ecomm/tomorrow/index_en.htm

Links to policy documents

- **Digital Agenda for Europe - COM(2010)245 of 19 May 2010**
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

- **Proposal on ENISA - COM(2010)521 of 30 September 2010**
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF

- **Proposal for a Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA - COM(2010)517 of 30 September 2010**
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF

- **The EU Internal Security Strategy in Action - COM(2010)673 of 22 November 2010**
  http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf