



Cyber Security in the European Union

Antoaneta Angelova-Krasteva

**Unit A3 – Internet, Network and Information Security
DG Information Society and Media
European Commission**

antoaneta.angelova-krasteva@ec.europa.eu

10 November 2011, Brussels



What is the problem?

An evolving scenario – Threats and risks

Steady growth in number, scope, sophistication of attacks

2007	2008	2009	2010	2011	2012
Estonia	Lithuania --- Georgia ---		Stuxnet	Emission Trading System (EU ETS) --- French government --- EC and EEAS --- Sony --- DigiNotar	...? 10% probability of a major CII breakdown in the next 10 years - potential global economic cost of over \$250B (Source: WEF)

European Commission Information Security and Media



What is the problem?

Economic cost of attacks

A few key examples...

SONY

\$175M

EU ETS

€30B

Cybercrime in the UK

£27B/year

Global cybercrime: \$388B/year

Major attack against the EU would cause disruption to:

- **Electricity grids**
- **Critical Information Infrastructures**
- **Financial services and markets**
- **Communications networks and infrastructures**
- **The Single market**

E.g. The macroeconomic costs of a major disruption to Switzerland are estimated at 1.2% of GDP



Cyber security: the EU Policy

- Focus on **prevention, resilience and preparedness** (complementary to fighting **cyber crime**)
- Take into account the **civilian & economic stakeholders'** role and capability (role of private sector & the **governance challenge**)
- Make **security and resilience the frontline of defence**
- Adopt an **all-hazards approach**
- Develop a **risk management** culture in the EU
- Focus on the role socio-economic **incentives**
- Promote **openness, diversity, interoperability, usability, competition** as inherent security safeguards
- Boost a global **collaborative policy and operational cooperation** across the EU, in particular on CIIP



A Digital Agenda for Europe-COM(2010)245

The Seven Priority areas for action

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



Overview of Pillar 3 “Trust and Security”

- INFSO CdF
- HOME CdF
- Others COM CdF
- ◇ Commission action
- Member States action

Cybersecurity preparedness

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

Cybercrime

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

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



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

- Compared to the current Regulation, key changes introduced by the proposal to help ENISA carry out its missions
 - **More flexibility, adaptability and capability to focus**
 - **Better alignment with the EU regulatory process**
 - **Interface with fight against cybercrime**
 - **Strengthened governance structure**
 - **Simplification of procedures**
 - **Possibility to extend mandate of Executive Director**
 - **Gradual increase of resources**



CIIP COM(2011)163

“Achievements and next steps: towards global cyber-security”

- Adopted on **31 March 2011**
- **Takes stock** of results achieved since 2009 CIIP action plan
- **Builds** on existing policy initiatives, in particular **Digital Agenda for Europe, Stockholm Action Plan** and **Internal Security Strategy**
- **Highlights** next steps at **European** and **International** level



CIIP COM(2011)163

“Achievements and next steps: towards global cyber-security”

Reports on the achievements and next steps in the 5 pillars of the CIIP Action Plan:

1. Preparedness and prevention
2. Detection and response
3. Mitigation and recovery
4. International Cooperation
5. Criteria for European Critical Infrastructures in the ICT sector



CIIP COM(2011)163

“Achievements and next steps: towards global cyber-security”

- **Examples of achievements:**
 - 20 MS with **Nat/Gov CERTs** in place*.
 - To date, **12 MS*** have carried out **cyber-exercises** at national level
 - **Cyber Europe 2010** was carried out on 4th November 2010 with the involvement of all Member States, plus Switzerland, Norway and Iceland;
 - **7 EU MS** took part in **US exercise Cyber Storm III** (EC and ENISA observers);
 - **European principles and guidelines for Internet resilience and stability** developed within EFMS
 - Progress on **ICT criteria for European Critical Infrastructures**, identification of priorities for Internet resilience and stability, exchange of policy practises.

** Based on information provided to ENISA by MSs*



CIIP COM(2011)163

“Achievements and next steps: towards global cyber-security”

- Positive achievements but further efforts are needed and the EC calls upon MS to commit to:
 - Enhance EU preparedness by establishing a **network of well-functioning National/Governmental CERTs by 2012**;
 - A **European cyber-incident contingency plan** and **regular National and pan-European cyber exercises** by 2012;
 - **European coordinated efforts in international fora** and discussions on enhancing **Internet security and resilience**.

CIIP COM(2011)163

“Achievements and next steps: towards global cyber-security”

- **Global coordination is important and necessary**
- The Commission will:
 - Promote **principles for Internet resilience and stability*** developed within the EFMS;
 - Build **strategic international partnerships** (e.g. EU-US Working Group on Cyber-security and Cyber-crime) and pursue coordination in International *fora*
 - Develop **trust in the cloud**



CIIP COM(2011)163

“Achievements and next steps: towards global cyber-security”

- **CIIP Ministerial Conference** in Balatonfüred (HU), 14-15 April 2011
- **HU Presidency Statement** on the Conference was issued
- Political commitment to **more EU cooperation** and to **reinforce coordination and cooperation at the International level**
- **Council Conclusions on CIIP** adopted on 27 May



CERT for the EU Institutions

Goal: to help the EU Institutions to protect themselves against cyber threats

- A “[Rat der IT Weisen](#)” was established to provide recommendations on how to set up such a CERT
- 1 June 2011 – establishment of a [CERT Pre-configuration team](#)
- 1 September 2011 – the EU CERT Pre-configuration team became [operational](#)

www.cert.europa.eu



EU-U.S. Working Group on Cybersecurity and Cybercrime - *Priority areas*

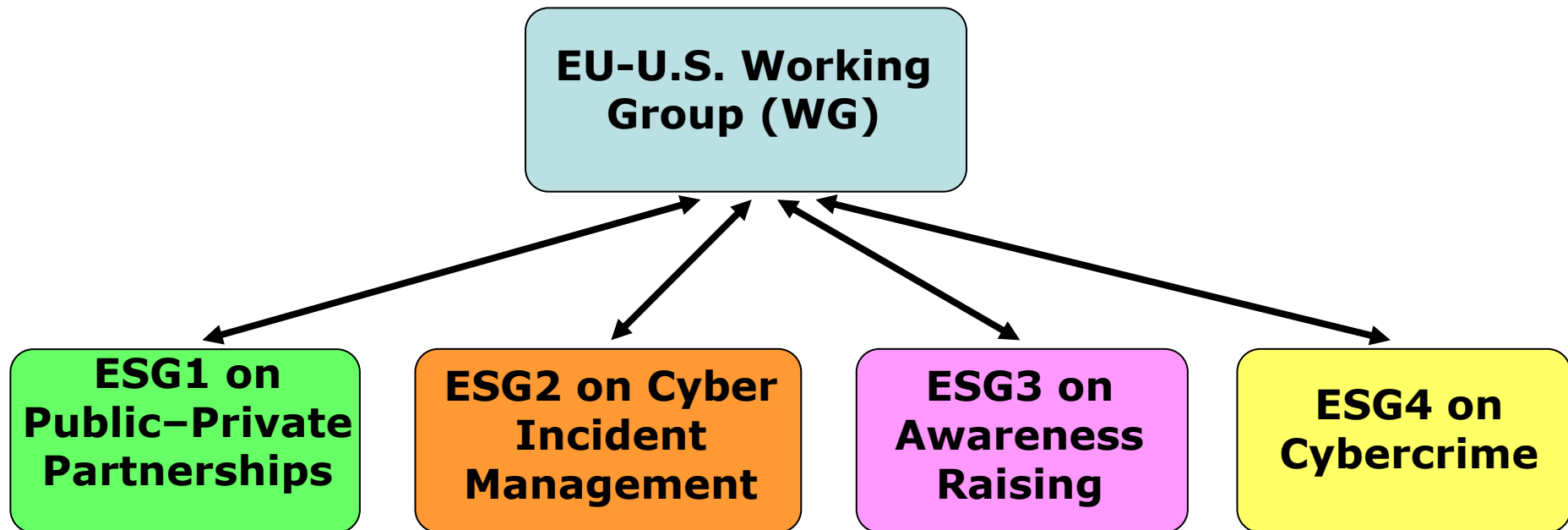
1. **Public – Private Partnerships (PPP)**
2. **Cyber Incident Management**
3. **Awareness Raising**
4. **Cybercrime**

➤ **Outreach to other regions or countries**

*To share approaches, avoid duplication of effort,
facilitate a joint approach in international fora*



EU-U.S. Working Group on Cybersecurity and Cybercrime - *Priority areas*



EU-U.S. Working Group on Cybersecurity and Cybercrime – *Coordination with EU Member States*

- **Political level:**
 - Discussions may take place at the level of the Council of the EU or in informal ministerial meetings
- **Technical and working level:**
 - For cybersecurity aspects, MS are primarily engaged via the EFMS
 - For cybercrime aspects, MS are primarily engaged via the European Cyber Crime Task Force (ECTF) which involves EU MS Heads of cybercrime units
- **Overall coordination:**
 - EU MS will be regularly informed via the Transatlantic Relations Working Group - COTRA



"Cyber Atlantic 2011"

- 3 November 2011 – the **first EU-US cyber incident exercise** took place in Brussels
- Participation from the US Department of Homeland Security, EU Member States, the European Commission, ENISA, the EU CERT.
- A table-top exercise, focusing on 2 scenarios:
 - a cyber-attack attempting to extract and publish online sensitive information from the EU's national cyber security agencies
 - an attack on supervisory control and data acquisition (SCADA) systems in EU power generation equipment



Future initiatives

- Call by the European Parliament for a truly strategic approach to cyber security issues
- The Commission is working on a comprehensive Internet Security Strategy to ensure that the EU and its Member States are adequately protected against cyber threats.



How should Europe be protected?

A European Internet Security Strategy

A comprehensive European Internet Security Strategy will include, *inter alia*, the following measures:

- All MS to have Public crisis response bodies (CERTs) in place
- All CERTs to become part of a network and cooperate effectively
- All MS to have strategies in place and contribute to a plan for EU-wide cooperation
- Obligation of reporting attacks



Web Sites

- **EU policy on Critical Information Infrastructure Protection – CIIP**
http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm
- **A Digital Agenda for Europe**
http://ec.europa.eu/information_society/digital-agenda/index_en.htm
- **EU policy on promoting a secure Information Society**
http://ec.europa.eu/information_society/policy/nis/index_en.htm

Links to policy documents

- **Commission Communication on Critical Information Infrastructure Protection – "Achievements and next steps: towards global cyber-security" - COM(2011) 163**
http://ec.europa.eu/information_society/policy/nis/docs/comm_2011/comm_163_en.pdf
- **European principles and guidelines on Internet resilience and stability**
http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf
- **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>