EP3R – The European Public Private Partnership for Resilience
Agenda

• About Public-Private Partnerships
  – Threats
  – Composition of PPPs
  – Information Exchanges

• EP3R
  – Approach
  – NEISAS
  – Traffic Light Protocol
Types of PPP

- Geographical – focused on a specific area within a Member State
- Sectoral – Finance, Water, Transport, Energy, Electronic Communications
- Cross-sector – e.g. Transport and Food
- Thematic – e.g. SCADA (Supervisory Control And Data Acquisition)
Types of threat addressed

• Natural hazards, e.g. floods, hurricanes, etc.
• Systems failures, e.g. hardware, software, loss of power, etc.
• Cyber crime, e.g. denial of service attacks
• Terrorism, e.g. physical attack, although possibly against another target
• Someone doing something really stupid
London bombings – July 2005
Walham 400kV substation – July 2007
Ilford (East London) – April 2009
The focus of PPPs

• Prevention-focused
  – Deter
  – Protect

• Response-focused
  – Detect
  – Respond
  – Recover

• Umbrella PPPs
  – Prevention and response focused
UK Electronic Communications Resilience & Response Group

• Industry:
  – Fixed-line telecommunications CSPs
  – Mobile telecommunications CSPs
  – The Internet peering community

• Government:
  – Central Government
  – Government Department with responsibility for electronic communications

• Other:
  – National Industry Regulator

• National Emergency Alert for Telecoms (NEAT)
UK NEAT successes

- March 2004 – Manchester tunnel fire
- July 2005 – London bombings
- December 2005 – Buncefield oil depot
- February 2007 – Cumbria rail crash
- July 2007 – Gloucester floods
- April 2009 – Ilford cable tunnel
- March 2010 – Paddington exchange flood
UK Exercise history

- 2005 – First full industry exercise – variety of scenarios
- 2006 – Severe weather in northern England and southern Scotland
- 2007 – Loss of power across south-west England
- 2008 – Planning team built a national plan for total loss of communications
- 2009 – Exercise “White Noise”
- 2010 – National loss of Internet connectivity
Examples of Information Exchanges

• UK
  – Network Security Information Exchange (NSIE)
• Netherlands
  – Telecom-ISAC
• EU-wide
  – EuroSCSIE (SCADA)
• USA
  – IT-ISAC
Benefits of PPPs

• They can help to implement a national security and resilience strategy
• Members can share information on emerging threats and new technologies
• Organisations can cooperate in times of crisis
• A PPP can reduce duplication of effort
• The whole is greater than the sum of the parts
Industry inhibitors

- Lack of trust
- Competitive fears
- Threat of regulation
- Lack of incentives
- Lack of perceived return on investment
- Travel and participation costs
EP3R Approach

• To build upon national initiatives between the public and the private sectors
• To seek the active contribution of relevant public and private stakeholders
• To prioritise the resilience challenges within the ICT sector
• To promote and pursue international cooperation
Building on national PPPs:

• Will broaden the levels of knowledge and experience for EP3R

• Will allow EP3R to use ‘best of breed’ ideas and methods

• Will allow Member States to lead the way, rather than being driven by regulation
Development towards EP3R

• Identify those PPPs who are willing and able to take a leading role
• Engage with the private sector across the Community as a priority
• Enable secure and reliable information sharing between PPPs
• Build on the success of Cyber Europe 2010 (the first Pan-European Exercise)
Some EP3R issues

- Not all Member States have relevant PPPs – encouragement is needed

- Not all PPPs do the same things in the same way – need to compromise rather than standardise

- Industry does not always see the value – plenty of work for little reward – incentives are needed
Some EP3R Inputs

• Good Practice Guides
  – Enabling and managing end-to-end resilience (2011)
  – Cooperative Models for Effective Public-Private Partnerships (later in 2011)

• National & European Information Sharing & Alerting System (NEISAS)

• Cyber Europe 2010
NEISAS

- Secure, nationally-based platforms, managed by TrustMasters in Italy, UK & the Netherlands
- Uses a common approach to Secure Information Sharing (ISO/IEC 27010)
- Supports the Traffic Light Protocol (TLP)
- Provides anonymity
- Supports Information Rights Management
- Permits cross-Border Sharing
- Watch the movie at www.neisas.eu/
Traffic Light Protocol (TLP)

- **RED** - Personal for Named Recipients Only - In the context of a meeting for example, distribution of RED information is limited to those present at the meeting, and in most circumstances will be passed verbally or in person.

- **AMBER** - Limited Distribution - Recipients may share AMBER information with others within their organisation, but only on a ‘need-to-know’ basis. The originator may be expected to specify the intended limits of that sharing.

- **GREEN** – Community-Wide - Information in this category can be circulated widely within a particular community or organisation. However, the information may not be published or posted on the Internet, nor released outside of the community.

- **WHITE** - Unlimited - Subject to standard copyright rules, WHITE information may be distributed freely and without restriction.
EP3R Thematic Working Groups

- **Working Group 1**: Identify key assets / resources / functions for the continuous and secure provisioning of electronic communications
- **Working Group 2**: Determine baseline requirements for security and resilience of electronic communications
- **Working Group 3**: Identify coordination and cooperation needs and mechanisms to prepare for and respond to large scale disruptions
References

• Availability and Robustness of Electronic Communications Infrastructures “The ARECI Study” Final Report, March 2007
• COM (2009) 149 Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience
• Resilient e-Communications Networks. Good Practice Guide Network Security Information Exchanges, ENISA, June 2009
• Cyber Europe 2010
EP3R Contact points

• Evangelos Ouzounis
  evangelos.ouzounis@enisa.europa.eu

• Lionel Dupré
  lionel.dupre@enisa.europa.eu

• The NEISAS url – www.neisas.eu/
Thank you