Resilience of Public Communication Networks and Services

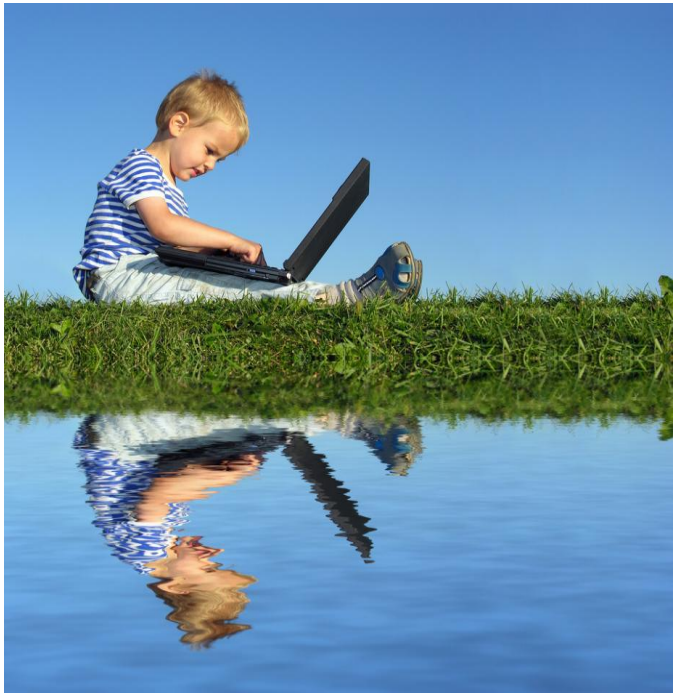
Dr Udo Helmbrecht

Executive Director
European Network and Information Security Agency (ENISA)

I International Critical Infrastructure Protection Meeting
Madrid, 18 February

Context

- communication networks & services are critical for economy & society
- constantly changing threat environment
- security and resilience a major challenge for all



Threat Environment

- significant physical disasters affecting CIIPs
- complex networks and services
- low quality of software and hardware
- asymmetric threats allowing remote attacks to CII
- increasing organised cybercrime and industrial espionage
- lack of international agreements and regimes,
- lack of well functioning, international operational mechanism

Our Challenges

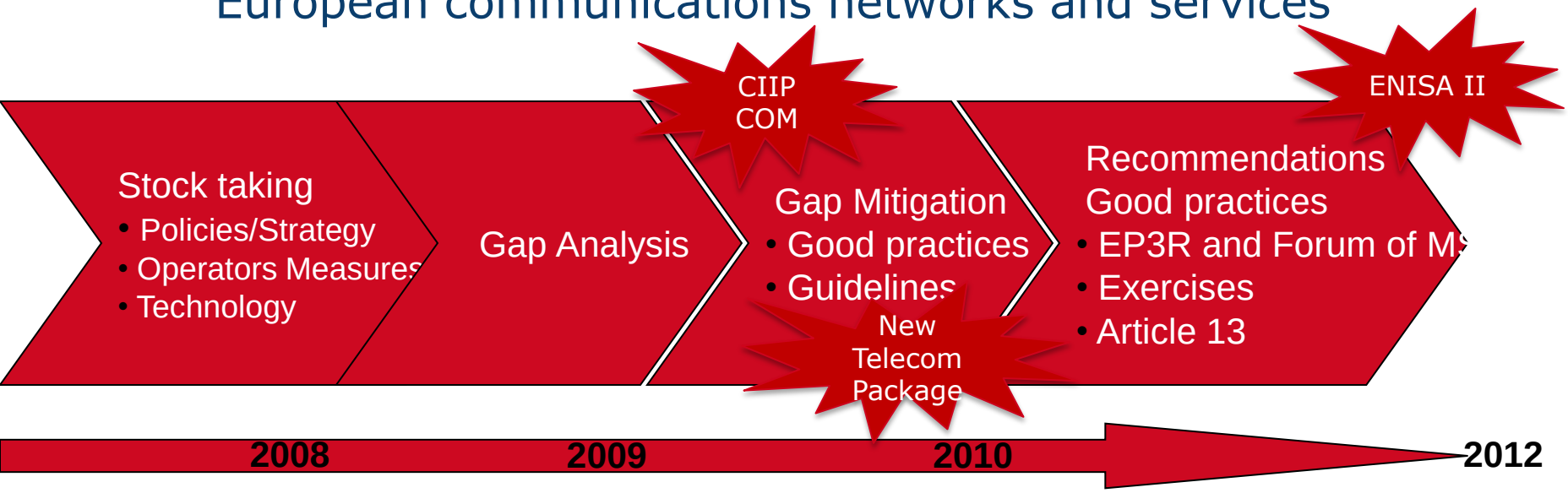
- CIIP - global issue without global governance
- uneven and uncoordinated national & European activities
- insufficient co-operation among private and public stakeholders
- lack of holistic cyber security strategies
- lack of efficient Information sharing & good practice guides
- insufficient experience in national and pan European exercises

EU Activities on Resilience and CIIP

- **CIIP Action Plan**
  - **Preparedness & Prevention**
    - Pan European Public Private Partnership for Resilience (EP3R)
    - Pan European Forum for Member States
    - Baseline Capabilities of National/Gov CERTs
  - **Detection and Response**
    - European Information Sharing and Alert System (EISAS)
  - **Mitigation and Recovery**
    - Pan-European exercises on large-scale network security incidents
    - National Contingency Plans
    - Reinforced cooperation between National / Governmental CERTs
  - **International cooperation**
    - principles and guidelines on long term Internet resilience and stability
- **Telecom Package**
  - **Article 13, Reporting Serious incident to NRAs and ENISA**
- **ENISA II – new mandate**

ENISA's Resilience and CIIP Program

collectively evaluate and improve resilience of European communications networks and services



EU Commission and at least 50% of the Member States made use of ENISA recommendations in their policy making process

12 High Level Recommendations I

- holistic and integrated national cyber security strategies
- need for a consistent pan European policy and strategy
- soft-law instruments (e.g. guidelines, recommendations, good practices)
- one State = 1 national/Gov CERT
- one State = one regular bi-annual national exercise
- one pan European exercise every 2 years

12 High Level Recommendations II

- one State = national contingency plans
- holistic and integrated national risk management processes
- establish national trusted information sharing schemes
- adherence of operators to preparedness measures and good practices
- cost effective incident reporting procedures based on good practices
- deployment of more secure technologies (IPv6, DNSSec, BGPSec, etc.)

Good Practice Guides and Results I

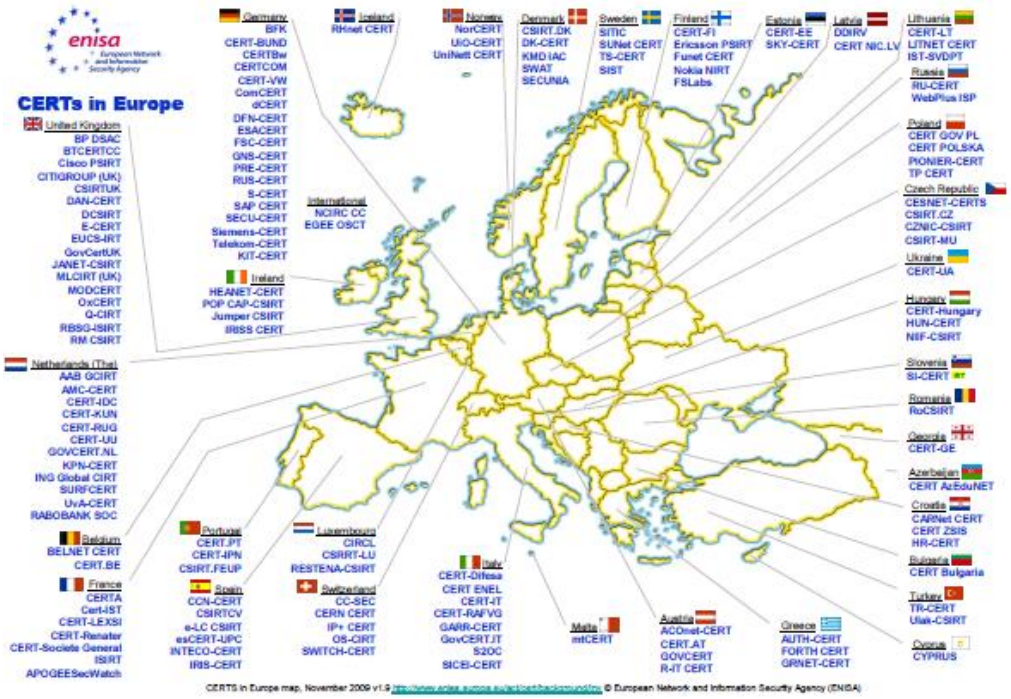
- **Information Sharing**
  - PPPs among private and public entities
  - sharing information on serious threats & vulnerabilities
- **Incident Reporting**
  - a practical guide to set up an incident reporting scheme
  - a solid basis for implementing article 13 of new Telecom Package
- **National Exercises**
  - a practical guide to set up national exercises
  - basis for the first pan European exerise
- **Stock Taking and Analysis of MS' Regulatory and Policy environments**
  - analysis of 25 national reports on policy, regulatory and operational environments
- **Providers Measures**
  - analysis and good practices on mutual aid assistance, business continuity, third party dependencies

Good Practice Guides and Results II

- **DNSSec Deployment**
  - good practices guide on how to deploy DNSsec
  - cost benefit analysis, trusted anchor repositories
- **Cloud Computing**
  - cloud computing recommendations and assurance framework
- **Priorities of Research On Current and Emerging Network Trends**
  - research trends, R&D areas and priorities for EU funded R&D Programs
- **Identification of standards**
  - gap analysis of existing standards
- **CERT baseline capabilities**
  - gap analysis of typical CERTs services

CERT situation in Europe – an overview

- **Number of national/governmental CERTs grows, but still there are gaps**
- **Capabilities of national / governmental CERTs still vary a lot among the Member States**
- **Cross-border cooperation among teams exists, but can be improved**
- **CERT responsibility / tasks grow!**



http://www.enisa.europa.eu/act/cert/background/inv

Highlights of 2010 Priorities

- implementing measures for reporting serious security incidents (article 13)
- first pan European Exercise
- metrics and data collection
- botnets
- DNSSec
- Secure routing and interconnection
- end to end secure architectures

Conclusions

- security & resilience of CII extremely important
- uneven and uncoordinated national & European activities
- Com's Communication on CIIP and Telecom Package reform a milestone; paves the way for a holistic pan European strategy
- strategic Public & Private Partnership is needed to enhance co-operation among public and private stakeholders
- ENISA's role stronger than ever to meet the challenges

Contact

Dr Udo Helmbrecht
Executive Director

European Network and Information Security Agency
Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

udo.helmbrecht@enisa.europa.eu

www.enisa.europa.eu