Emergency Preparedness in the field of fixed and mobile telecommunications and Internet

WORKSHOP  ExTrABIRE
Roma, June 13, 2011

Sandro Bologna
AIIC President

www.InfrastruttureCritiche.it
AIIC è un’associazione scientifica senza fine di lucro che nasce nel luglio del 2006 per promuovere e sostenere una cultura interdisciplinare per lo sviluppo di

- Strategie
- Metodologie
- Strumenti
- Tecnologie

per la protezione di infrastrutture critiche, specialmente in situazioni di crisi
AIIC – Associazione Italiana esperti Infrastrutture Critiche

Convegni e workshop

Colloquia sulle Infrastrutture Critiche

Sito web e newsletter

Alla Rivista di Divulgazione scientifica
THE PROJECT

JLS/2008/D1/018
A study on measures to analyse and improve European Emergency Preparedness in the field of fixed and mobile telecommunications and Internet

Principal investigators:

*Paul Theron, Fabien Cavenne: THALES GROUP - FRANCE*

*Hanne Henrotte: ALCATEL-LUCENT*

*Chirs Johnson: University of Glasgow*

*Sandro Bologna: ENEA*
Project Key questions

- What is the definition and scope of preparedness?
- What are the preparation procedures / process currently in place throughout Europe, at the level of Operators and Member States (as well as between Member States)?
- What are the mechanisms by which preparedness is achieved?
- How do stakeholders exchange and share their good practices in that area?
- What are Operators and Member States' priority procedures should an emergency occur?
- What level of support and involvement do Member States commit to facilitate - and benefit from - Operators' Emergency Exercises?
**Project Aims**

- Identifying and evaluating how preparedness is achieved in the field of European fixed, mobile and Internet communications.

- Proposing elements for future policies, measures and guidance designed to improve the level of preparedness and co-operation within the Telecommunication sector on a European scale.

- Promoting cross-border co-operation between Member States and Operators in order to address large scale emergencies (i.e. bearing on two or more States or extending beyond the limits of the Union).

- Making the conclusions of the study known to Operators, Member States and Stakeholders.
**Preparedness**

- The state of readiness to cope with, or to support others in a major disruption, i.e. the level of potential resilience that an organisation has reached through a preparation loop.

**Preparation Loop**

- The process chosen by Stakeholders, Member States or the EC in order to prepare for Emergency Situations through preparation activities.

**Emergency Preparedness**

- Emergency Preparedness aims at getting ready for « the unexpected » - not for everyday incidents.
The Preparation Loop

Re-assessment → Policy

Practice → Elaboration

Dissemination → Education

Feedback → Exercising

Preparation Loop

Figure 4-1: The Preparation Loop and its activities
Steps in the Preparation Loop

- **Re-assessment** of existing practices vs. reassessed needs, legislation and goals
- **Policy Definition** to frame future Preparation efforts
- **Elaboration** of dispositions and good practices
- **Education** of operators, suppliers and stakeholders' staff
- **Exercising** (tests performed in-house, nationally, cross-sector, cross-border)
- **Feedback** from experience (both from real crises & from exercises)
- **Dissemination** of knowledge and experience to the community
- Learning by **Practice** at stakeholders' level (European agencies, national governments, operators, ...).
PROJECT FINDINGS (1/2)

Emergency preparedness

- Generic definitions, depends on stakeholders’ perspective
- No shared definition
- No precise lists of activities

- Emergency Preparedness can not be the fact of the Telecommunication sector only because of the manifold interdependencies it has with so many other critical sectors: “Telecom Inclusion Principle”

- Pan-European Exercises are needed but currently seen as a target still remote
PROJECT FINDINGS (2/2)

Regulations

- No Hard Regulation at the International & EU
  - COM(2011)163 of March 31st 2011

- A bit more at National level
  - CIP/CIIP national regulation (France, Germany, ...)
  - Business continuity requirements from governments
  - Emergency preparation instructions (Finland, Sweden, ...)

- Adverse effects of regulation (market deregulation)

- Regulation is a slow mover compared with fast paced technology

- The concept of “Circle of Absolute Trust” to foster collaboration in Emergency Preparation and cooperation in Emergency Response
Interdependence vs Preparedness Plans

From Project Final Report:

“A lot of respondents recognize that very little has been done, so far, regarding interdependency and coordination across telecommunication and other CI sectors.”

ICT stakeholders are aware of their dependence on Electric System and other services; their Preparedness Plans foresee “Backup Solutions” but do not consider overall interdependences.
Interdependence Loops

ICT Stakeholders are aware of their dependence on Electric System and usually adopt autonomous prevention measures such as UPS.

Upon Outages, UPS devices actually delay the misbehaviour, while transferring dependence from ES to Transport and Fuel Distribution which, in turn, depend both on ITC.

The current preparedness plans do not consider interdependencies because the preparation process does not include interdependence modelling.

Inter-dependence means non trivial loops

- Electric System
- Telecom Operator
- Transports
- UPS
- Fuel
The Preparation Loop

The interdependency issue should be considered at the Policy level in order to set a proper Emergency Preparedness.

Figure 4-1: The Preparation Loop and its activities
Conclusions

- No common definition of Preparedness Plan
- No common regulations
- Interdependence represents a key issue for the security and the preparedness.
- Presently Preparedness Plans are not coordinated among operators and hence unable to face contingencies involving inter-dependencies.
- A Shared Risk vision is required to deal with real large contingencies.
- The elective means to provide Shared Preparedness Plans is Public-Private Partnership.
- An appropriate Preparation process should involve experts from all the different technological Asset Owners.
FURTHER READINGS

Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM (2009)149:


European principles and guidelines for the resilience and stability of the Internet