

# **Summary report of stakeholder meeting on availability and robustness of electronic communication networks**

**Brussels, 18 June 2007**

## *Introduction*

This joint stakeholder meeting on availability and robustness of electronic communication networks was attended by approximately 60 representatives from government, authorities and private industry and their representative organisations. The meeting followed on the publication of the final report by Alcatel-Lucent on availability and robustness of communication networks in April 2007 (the ARECI report) [link ARECI report and annexes] and a period of consultation during which stakeholders were given the possibility to comment on the report. The main aim of the meeting was to present and discuss the comments made to the ARECI report.

The meeting was opened by Mr. Servida (European Commission, DG Information Society and Media, chairman), setting out the political context of the Commission's work on availability and robustness of electronic communications networks. He referred to the Commission Communication on a secure Information Society [link to Communication and the Council Resolution] and the proposed European Programme for Critical Infrastructure Protection [link to EPCIP GP and proposal for Directive]. He introduced the agenda of the meeting [link to agenda].

## *Presentation*

During the morning session, presentations were given of their written comments by the speakers as indicated in the agenda.

Commentators and speakers generally found that the ARECI report is important, relevant and worthy of support. They recognise and acknowledge the value of the information provided in the report. The Recommendations receive broad support except for the recommendations (7 and 8) on standardisation and interoperability testing respectively where most commentators felt that industry should lead and issues should be left to the market.

Wide support was also received for the Commission's initiative that would need to lead to more commonality in the approach across Europe. To this end, several commentators said that a growing number of Member States are preparing their own approach and stressed the need to act now as otherwise industry will be faced with various incompatible approaches and barriers to trade.

The written comments and the presentations (where available) can be found on this website [[link to written contributions and presentations](#)].

### *Discussion*

In the afternoon, an open discussion took place with a view to seek answers on some key questions:

- Where could a European approach add value to Member State and other stakeholder initiatives?
- What should a multi-stakeholder dialogue look like?
- What are the issues you would like to see being addressed?

The comments and discussion provided a breadth of further issues not covered by the ARECI report. Many of these issues are related to the new broadband online environment and to what is needed for its protection. Some new issues shed a new light on the matter or provide a wider perspective. They are set out in the Annex.

During the discussion the broad lines of a consensus seemed to develop on the following points:

- There is room and in fact need for a multi-stakeholder dialogue on availability and robustness of electronic communications networks in Europe; this dialogue becomes increasingly urgent because a growing number of Member States is preparing their own approach.
- To this end, it would be useful to do some stock taking i.e. to produce an inventory of who does what in Europe (initiatives in Member States, what public-private-partnership structure and drivers); to (develop mechanisms to) analyse what has been achieved at national level; and to see whether such existing good practices can be and would usefully be replicated at the European level.

A work order for ENISA to carry out a survey of the existing national regimes concerning the obligations and requirements on network operators and/or service providers to ensure and enhance the security and resilience of public communications networks is currently under discussion.

However, our overall assessment is that comments made in writing and during the meeting reveal different backgrounds, different roles and responsibilities, and different interests and expectations of respective commentators. Also the very wide range of issues arising from the ARECI report and from the comments made, made it impossible to keep focus on the questions posed or to find a common line or shared understanding on the issues at this stage.

*Final remarks*

This was only a first joint meeting of stakeholders with different backgrounds, responsibilities and perhaps expectations. Only through prolonged informal multi-stakeholder dialogue involving all stakeholders will it be possible to develop a shared understanding of the issues at stake and reach a consensus on the European agenda.

In the next few months, we will expand our analysis and prepare a discussion paper to guide further discussion with the stakeholders on this matter during the Autumn of 2007.

## **Annex: Further issues raised**

1. Presentations and discussion revealed that different views are held on the model for information sharing in Europe: meshed or central. Where the ARECI report promotes a meshed system, others advocate a centralised system as the only manageable solution in a real time environment.
2. Commentators stressed that once good information sharing mechanisms are in place, then the difference between the governments' interests and firms' own self-interests are small. This strengthens our motivation for multi-stakeholder dialogue in Europe to enhance our shared understanding of the issues.
3. Commentators raised the point that multiple components and network elements, typical for the heterogeneous nature of future networks, place a burden on incumbent network operators. It is increasingly difficult to establish procedures leading to the identification of protection gaps and identify liabilities. A need was identified to develop security metrics via collaborative efforts.
4. It was pointed out that business' continuity plans are based on broadband access but the dimensioning is not compatible with plans and usage in fixed telecommunications covered by the ARECI report. The need for an overall IT risk management approach and an alignment of IT solutions with the risks was highlighted. While the ARECI report provides a complete list of ingredients that make up a communications infrastructure, in the new online environment with multiple levels of complexity security needs to be process driven, proactive, fast, flexibly and intelligence led. Present day organisations are not fast enough to deal with the new environment. Technological developments are taking place at such a fast pace that authorities and other decision making bodies have insufficient up-to-date expertise and information, and these bodies are in danger of implementing measures that are out of step with the actual threat situation
5. Participants said that the ARECI report is technical contents only. They emphasised the critical role of people and processes to make technology works and ensure ongoing effectiveness in the light of both changes in the online threat environment and the adoption of advanced modern technology by the emergency services. Also the importance of cultivating a trusted environment was often mentioned.
6. Although Internet service providers agree on the importance of identity management, they disagree with statements in the ARECI report on the need for federated identity management.
7. Commentators raised new issues such as outsourcing in a multi-vendor hardware/software stack and stressed the dependency on suppliers of equipment and installers. Open source was seen as very important for managing a national crisis.

8. Commentators said that the ARECI report does not cover mobile. But the number of mobile subscribers is twice the number of fixed subscribers while mobile networks may have special vulnerabilities including failure to power outages. National roaming for emergency service is mentioned as a possible measure to enhance availability.
9. In a presentation it was argued that there is a Business Case for security. Customers are willing to pay more if they realise how vulnerable they are. This dimension should be explored further.
10. In this same context, commentators saw a need to assess the economic aspects and cost effectiveness of the ARECI Recommendations. It is important to study the market/economic dimensions of resilient communications.
11. In the current systems, several commentators pointed to the risk brought through the dependency on software-controlled systems and technology. They suggest that the EU promotes systematic vulnerability analysis. It may be useful and provide added value to Member States and private industry to develop at the European level guidelines for systematic vulnerability and robustness testing and the hardening of (existing) software controlled systems
12. Commentators warned for the consequences of the trend of co-location where network operators and providers of applications and services are co-locating, for various reasons. Physical diversity can be compromised; the effect of a single failure has the potential for greater damage. There is a need to study the consequences collocation, co-trenching, duct sharing and the relative openness of the perimeter for personnel from different contractors to co-location sites.
13. It was further suggested that, in order to reduce dependencies of other critical services and supplies and key resources, it must be considered to build firebreaks and/or buffers to stop or slow down a domino effect.
14. Commentators also saw bias in the ARECI report against open source. But they argue open source may offer great benefits to critical infrastructure as it ignores the threats of a software monoculture. They further argue that several critical building blocks are missing from the report when considering the integrity of the supply chain while the report is contradictory in itself. A software monoculture and risk of non-access to source code pose big problems in times of national emergency or crisis.
15. Commentators pointed out the important role of terminal equipment / trusted computing in protecting networks. Linked to this is the ongoing de-perimeterisation in convergent architectures – there is no longer a single perimeter.
16. The mass scale susceptibility of DNS to attack was evoked together with the unwillingness by ISPs / countries to prepare for DNS poisoning.

17. Commentators mentioned the importance of studying and mastering both cross-sector and intra-sector (inter)dependencies as well as the cross-borders operations. In this respect, the focus for EU actions should be on interdependencies and interoperability.
18. The key role of testing / exercising for interoperability, security and crisis management as well as the need to develop Pan-European testing exercises were highlighted.
19. In order to avoid duplication, future actions shall build on and engage existing communities (e.g. FIRST, ISPs etc.).
20. There is a need to deepen the understanding of CIIP issues, in particular with respect to interdependencies. To this end, the importance of well coordinated, structured and interdisciplinary R&D was evoked.
21. Importance of awareness raising towards:
  - national/European policy makers
  - intra-sector
  - people (education, schools, etc.)
22. The primary objective of EU actions should be to develop and make available principles to define critical functionality and services as well as good practice guidelines, and not necessarily to develop regulation.
23. There is a need for more pro-active and intelligence based approaches and actions to both resilience and robustness of information infrastructures as well as CIIP.
24. The importance of the "converged" perspective in addressing CIIP was evoked. The "convergence" (at all levels) have changed the horizon and made all networks to be interrelated:
  - not separate infrastructures (IP, service, etc.)
  - not separate networks (fixed, mobile, IP, etc.)
25. The focus of actions on resilience and CIIP should not be on "infrastructures" but on "critical services". What really matters is to ensure business and service provisioning continuity. To this end, "critical services" for business continuity should be defined. By so doing, policy initiatives and actions would primarily focus on benefits and not only on security issues as a whole.