



Brussels, 02 April 2008

WORK PAPER

**SUMMARY OF THE RESPONSE TO THE EUROPEAN
COMMISSION'S INVITATION TO COMMENT ON THE
AVAILABILITY AND ROBUSTNESS OF ELECTRONIC
COMMUNICATIONS INFRASTRUCTURES STUDY**

DISCLAIMER

**This report/document does not necessarily
represent the views of the Commission**

CONTENTS

1. OVERVIEW.....	2
2. SUMMARY OF THE COMMENTS RECEIVED	4
2.1. Comments concerning the ARECI study in general.....	4
2.2. Comments on the recommendations.....	5
3. ANNEX – LIST OF CONTRIBUTORS	13

1. OVERVIEW

In the 2006 Communication on "A strategy for a Secure Information Society – "Dialogue, partnership and empowerment""¹, the Commission characterised security and resilience of communication networks and information systems as a key policy priority for the European Union (EU). In that context, the European Commission has announced in the *Commission Legislative and Work Programme 2008*² a European policy initiative on Critical Information Infrastructure Protection (CIIP). The objective of this initiative, within the broader framework of the European Programme on Critical Infrastructure Protection³, is to ensure that adequate and consistent levels of **preventive, detection, emergency and recovery measures** are in place. To this end, the European Commission intends to engage relevant stakeholders and to build on national and private sector activities.

As a first step towards an EU policy initiative on CIIP, the European Commission engaged, in 2006, in a study on the *Availability and Robustness of Electronic Communication Infrastructures* (ARECI)⁴. The main findings of this study were presented to a broad audience comprising representatives of governments, industry and users on the 18 January 2007 and later on the Commission invited all interested parties to comment on the study's findings. Sixteen contributions drawing up comments on the ARECI study and its ten recommendations for enhancing the availability and robustness of electronic communication infrastructures have been received from a variety of stakeholders. The respondents include industrial associations in the fields of Telecommunications, Internet Services, Network and Information Security (NIS) and Critical Infrastructure Protection as well as individual operators or providers of electronic communications networks and services, one NIS products and services provider, two Member State authorities, one political party, two European Union specialised centre/agency and a standardisation body.

Most contributors welcomed European Commission's initiative on critical communications and information infrastructure protection and considered the ARECI study an interesting step on promoting these issues. The outcomes of this study were not only considered valuable, important and relevant, but also seen as an excellent basis for discussion. However, while the report proposed solutions and recommendations, the details to guide their proper implementation are missing. For instance, when describing the next steps the term "Private Sector" does not discriminate between infrastructure operators, service providers, software producers or hardware providers. The study was also considered to be too focused on the traditional communication infrastructure leaving out of the discussion technologies such as Internet, mobile and broadband access and to some extent what will be the basis of future networks.

¹ See COM(2006) 251, 31.05.2006 at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0251:EN:NOT>

² See COM(2007) 640, 23.10.2007 at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0640:EN:NOT>

³ See COM(2006) 786, 12.12.2006 at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0786:EN:NOT>

⁴ The study was carried out by Alcatel -Lucent's Bell Labs and Professional Services. See the final report at: http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3334

Comments on the recommendations

The importance of developing priority restoration procedures and emergency plans in partnership with all the stakeholders has received clear appraisal. However, it was commented that such emergency preparedness should be part of the development of business continuity plans, while emergency exercises should be taken into account within a Risk Management framework addressing large dependable systems.

Although telecom operators agree with the recommendation on implementing priority communications capability on public networks, it is mentioned that some solutions have been already implemented by telecom operators in some Member States. It was also noted that prioritization challenges are quite different between circuit switched and packet switched networks. In addition the rationale to invest on software or hardware upgrades in order to deliver priority communications on public networks is unclear.

Even though formal mutual aid agreements between industry stakeholders to enhance European networks robustness in crisis situations were welcomed, its practical implementation is considered as not straightforward due to a number of reasons such as the differences in legal systems, the involved costs and the challenge of cross-ownership.

The recommendation on critical infrastructure information sharing was very well supported, although contributors believe it is important to clearly identify several issues in order to enable secure and protected information sharing: scope, stakeholders and their respective responsibilities, format of the information to be exchanged and legal protection.

The recommendation on inter-infrastructure dependency studies and the one on a testing framework to connect new networks to existing ones were supported, even though both recommendations were considered quite generic.

The recommendations on supply chain integrity and unified European voice in standardisation were the ones generating more controversy among contributors, especially due to concerns on competition issues and innovation hampering.

Almost all stakeholders agreed that public-private partnerships should be promoted, provided that some elements like equity, common agreed approaches and confidential information sharing are in place. Some contributors noted that voluntary commitment between stakeholders on these issues can sometimes lead to better results than regulation enforcement.

Despite being considered costly, the implementation of the recommendation on sharing and using expert best practices was supported by all the contributors.

Eventually, the recommendations on information sharing, public-private partnership and the use and sharing of industry-consensus best practices were considered as inter-linked.

2. SUMMARY OF THE COMMENTS RECEIVED

This section analyses the comments received from sixteen contributors (listed in Annex 1) regarding the ARECI study in general as well as its ten recommendations.

2.1. Comments concerning the ARECI study in general

Most contributors welcomed European Commission's initiative on critical infrastructure and considered the ARECI study an interesting step on promoting these issues. The outcomes of this study were not only considered valuable, important and relevant, but also seen as an excellent basis for discussion. A better definition of some concepts, roles and responsibilities and the exchange of best practices were recognised as particularly valuable topics. Incumbent telecom operators highlighted the importance of coherent action across all sectors and countries, the need to respect proportionality and complementarities, and to create a level playing field among all operators.

In terms of further steps, a Member State suggested the creation of a European coordination organisation for the execution of the proposed measures and for ensuring the proper level of confidentiality. Two Member States made reference to regulation while asking for clarification on the link between the study and the revision of the Regulatory Framework for electronic communications networks and services and while suggesting the further elaboration of a European regulation to clarify responsibilities and encourage participation of all stakeholders.

Some respondents considered, however, that the study was unfortunately too generic for what concerns the findings, recommendations and required commitments leaving room for interpretation. They pointed out that several aspects were not tackled with enough details to further guide appropriate implementation, in particular the recommendations lack details on timing, costs and stakeholders involved in the implementation. Two respondents also underlined that the term "robustness" does not seem to be a widely term used in industry and it was difficult to understand its application extent in the study. Some contributors from the Network and Information Security industry also emphasized that the study was too focused on traditional communication infrastructures rather than on future networks. Therefore some suggestions of topics that should not be excluded from European Commissions' CIIP activities included Internet, mobile and broadband access and accessibility in emerging technologies.

A respondent directly involved in NIS activities also suggested, as an additional recommendation, that research on Risk Management/Risk Analysis methods addressing large dependable systems and governance of e-communications systems should be fostered. Other respondents involved in NIS activities pointed out the importance of raising awareness on the role of security processes and procedures and of setting up a systemic security management approach to achieve an effective protection of the communication and information infrastructure.

Respondents also addressed other issues in their contributions as follows:

- A telecom operator considered that the identification of critical infrastructure should be taken forward by Member States based on uniform criteria established across

European Union. Infrastructure interdependencies and vulnerabilities of all the players involved in the implementation of the recommendations should also be identified further.

- A respondent considered that the study is biased against Open Source and noted that ignoring Open Source's benefits to critical infrastructure would be a grave mistake. It was also mentioned that the threats of software monoculture were ignored in the report and information systems warfare issues were not specifically addressed.
- A respondent directly involved in critical infrastructure protection welcomed a strategy for raising awareness for planning and investing on critical infrastructures and emergency response. It also supported measures that would lead to an increased harmonization of disaster recovery arrangements across borders, standards, and general policy and regulatory frameworks. Furthermore it was mentioned that there are niche players willing to offer services needed to fill the gaps identified by the ARECI study in terms of preparedness, resilience and prioritization, arguing against the ARECI report statement that normal market forces are not at play in this area.

2.2. Comments on the recommendations

Recommendation 1 – Emergency Preparedness

The Private Sector and Member State governments should jointly expand their use of emergency exercises and establish pre-arranged priority restoration procedures for critical services to better meet the challenges of inevitable emergency incidents.

Telecom and mobile satellite operators supported this recommendation and noted that emergency exercises and priority restoration procedures already exist in most Member States. Nevertheless it was mentioned that the adoption of this recommendation would permit the improvement of the coordination and communication between stakeholders in emergency situations and would contribute to reinforce the idea that all stakeholders should have emergency plans. Moreover it was suggested that Member States should define pre-arranged priority restoration requirements and the private sector should be free to meet these requirements in terms of emergency preparedness according to its know-how. It was also emphasized the importance of interdependencies studies between stakeholders and between infrastructures.

Network and information security (NIS) providers also supported this recommendation and reiterated the importance of developing priority restoration procedures and emergency plans in partnership with all stakeholders involved in the ICT Sector (including Internet) together with industry partners. It was also recommended the creation of “Concept of Operations” (CONOPS) documents to set the procedures and the roles of all parties in case of an emergency. An industry association suggested that the European Commission could play an important role in setting up a secure repository of information regarding analysis of emergency incidents and promoting sharing of best and worst practices.

Other respondents remarked that joint emergency exercises are just one phase of a Risk Management framework and that most of the value of exercises comes from learning

how to get ‘people’ and ‘process’ issues right and find unexpected dependencies, rather than from the specifics of the scenario.

A respondent in the field of Internet services showed a sceptical view on the outcomes of the recommendation. First of all, it was not clear to what “critical services” were referred to – whether communications infrastructures or other critical sectors. Secondly, emergency preparedness was considered, to some extent, as part of business continuity planning and consequently the private sector should be encouraged to develop such plans accordingly. Finally, in its view it was not clear to what extent emergency exercises and priority restoration exercises contribute to the enhancement of robustness. A European body shared the same opinion on the generic approach of this recommendation – there is a need to clearly identify the meaning of emergencies and the role of each stakeholder.

Respondents also raised other issues that are worth noting:

- Who will bear the costs of emergency exercises, especially cross border ones that will require a significant investment;
- EU and Member States should foster Research on Risk Management/Risk Assessment methods to address large dependable systems;
- One respondent noted that this topic is also covered by the Public Safety Europe forum initiatives and therefore its activities should be taken into consideration.

Recommendation 2 – Priority Communications on Public Networks

Member State governments should implement a standards-based priority communications capability on future public networks in order to ensure vital communications for critical government authorised callers. This public network capability is needed in addition to any private emergency networks that already exist and should not be viewed as a substitute or replacement for such private networks.

Regarding this recommendation, although telecom operators agreed with it, it was also mentioned that some solutions are already implemented in several Member States. However, while one operator argued that there is no need for an EU-wide cross-border standard because bottlenecks usually have local dimensions, another operator stated that European and worldwide interconnection and interoperability of priority communications capabilities must be ensured. NIS providers supported the recommendation and reiterated once again the importance of involving industry players, as they can be vital in restoring critical communication infrastructure and noted that it is important to identify backup communications options, such as wireless and satellite, in the case that it is not possible to access the standard public network especially in case of emergency.

A respondent in the field of Internet services drew attention to the fact that prioritization challenges are quite different between circuit switched and packet switched networks. They also remarked that in some Member States, the physical separation between private emergency networks and public networks is not obvious. A respondent mentioned that "*Private networks used for emergency services do use resources common to public networks (for example, separate lines may be present within the same cabling). Therefore, private emergency networks probably rely on the infrastructure of public networks, which does impact the security of these networks*".

A respondent directly involved in NIS activities also underlined that most networks are run by the private sector, so what actually Member States can do is to request or regulate priority communications on such networks, instead of "implement" as stated by the recommendation. An operator even mentioned that Member States authorities should not implement but instead authorise standards-base priority capabilities. Another respondent also pointed out that there is a need to clarify the business rationale to invest on such prioritization, considering the involved costs on software and infrastructure upgrades.

Moreover, a respondent emphasized that prior identification of critical infrastructure is needed in order to implement prioritization for communications and actions. It was also raised by a contributor that the challenges for managing the lists of priority users are organisational rather than technical.

Other concerns raised by respondents include:

- The type of priority needed/implemented on public networks should depend on the specifics of the infrastructure involved and the emergency situation;
- A telecom operator drew attention to the fact that the implementation of this recommendation should not represent a financial burden for telecom and network operators and should rather be subsidized by Member States;
- Another respondent pointed out that the recommendation as stated implies that all emergency calls from any stakeholder will be prioritized and if this is put in place as a requirement for the European communications infrastructure, a complex agreement between service providers, equipment suppliers and regulators has to be foreseen on the definition of the networks' architecture and on which networks prioritization should be implement first;
- Other solutions different from implementing priorities on public networks are:
 - (a) Creating ad-hoc peer-to-peer public networks;
 - (b) Set-up a dedicated emergency network owned by the Member States (even if the operations are delegated to an operator) onto which all operators could connect their operations.

Recommendation 3 – Formal Mutual Aid Agreements

The Private Sector should establish formal mutual aid agreements between industry stakeholders to enhance the robustness of Europe's networks by bringing to bear the full capabilities of the European communications community to respond to crises.

Although most of the contributors welcomed the idea expressed in this recommendation, they stated that its practical implementation would be difficult to achieve due to a number of reasons such as different legal systems, costs involved, jurisdiction, cross-ownership, cross-border systems and so on.

Therefore, three approaches were proposed. Firstly, a study on the legal implications of such agreements before putting them in place was proposed. Secondly, it was suggested that instead of establishing mutual aid agreements based on abstract definitions of threats

and vulnerabilities, preparatory risk and business continuity assessments based on an asset-oriented approach should be carried beforehand in order to create more focused mutual aid agreements. Thirdly, a respondent had put forward that what is needed is a cooperative approach (for instance through the creation of public-private partnerships, communication protocols, information exchange or preparedness/assistance schemes) among industry, government and law enforcement, enabling greater flexibility and scope to develop effective and responsive relationships.

Besides these proposals, telecom operators suggested that Member States should commit the necessary funds to put this recommendation forward and that precise equipment standards are needed, especially in the IT world to make such mutual aid agreements effective. It was also added that equipment suppliers should comply precisely with those standards. A respondent directly involved in NIS activities highlighted that Member States and European Institutions could support the introduction of mutual aid agreements by fostering relevant public research, setting incentives and enabling operators of various sizes to participate in such agreements. Additionally, it supported the idea that such agreements should focus on a European perspective, ensuring uniform application of agreed definitions and standards in all Member States, and foresee specific procedures for cross-border transactions in crisis situations. However cross-border cooperation was considered more problematic by another respondent.

Recommendation 4 – Critical Infrastructure Information Sharing

Member States and the Private Sector should establish formal means for sharing information that can improve the protection and rapid restoration of infrastructure critical to the reliability of communications within and throughout Europe.

Although it was supported that information sharing is needed, there were two positions on how it should be set in place whether as a formal or informal means.

On one hand, most telecom operators, NIS and Internet service providers supported the view of formal information sharing. In particular, it was stressed the need for authorities, namely Law Enforcement Agencies, to participate in such information sharing, and to ensure information confidentiality. Moreover, telecom operators mentioned that such practices are already common practice among some operators and Member States. NIS providers also noted that information sharing should not be seen as a one way street but as a shared responsibility between all stakeholders involved and consequently it is vital that legal protection is set in place in order to enable secure and protected information sharing within Member States and cross-borders from legal prosecution.

Two other respondents drew attention to the fact that generally there is willingness to share information but lack of motivation to do so unless there is a clear incentive, especially in the case of higher maturity level stakeholders. Additionally, although two respondents directly involved in NIS activities agreed that a star topology is not appropriate for reasons of trust and could possibly create obstacles, they did not fully agree with a full mesh architecture. One contributor highlighted that an element of European coordination would still be necessary, and the other considered that the number of connections among different infrastructures (and consequently stakeholders) would be an obstacle and would end providing only a partial view of the online threat environment that an operator would have access to. Another respondent also remarked that one-to-one

links will most probably never result in effective information sharing and the creation of a new "European Institution" is not the solution to put forward. The need for a common "language" to describe security incidents, response and escalation that can be used across sectors and borders was also pointed out by respondents.

On the other hand, two other respondents supported the view that information sharing should be based on a secure and confidential voluntary forum instead of formal means. But, it should be left to Member States to evaluate if voluntary sharing is sufficient or if formal means are necessary.

Recommendation 5 – Inter-Infrastructure Dependency

European Institutions and Member States should engage with the Private Sector to sponsor a coordinated European-wide program that identifies and addresses the interdependencies between the communications sector and other critical sectors, to enhance the availability and robustness of Europe's public communications networks.

Most of the contributors strongly supported this recommendation, though some of them considered the proposed recommendation quite generic as it is stated. Therefore, to consider these interdependencies specific common approaches among Member States were proposed:

- Support the assessment of the reliability of the electronic communication infrastructure as part of any business continuity plans;
- Promote impact analysis where proper risk assessment is carried out in order to identify all interdependencies (both internal and external) including hidden and indirect interdependencies;
- The starting point for such an analysis should be at national level;
- A wide view needs to be taken on the scale and scope of potential interdependencies.

A contributor, however, underlined that the need for a European-wide programme should be better justified since studying interdependencies can be approached by good industrial practices. It also stated that unless such interdependencies are directly linked to specific critical situations, the proposed action will rarely contribute to the enhancement of availability and robustness of Europe's critical infrastructures.

Some contributors also addressed the requirement of public funding as the driver to put this analysis rolling because no single organisation could afford such costs.

Recommendation 6 – Supply Chain Integrity and Trusted Operations

European Institutions and Member States should embark on a focused program to promote the integrity of supply chains used to build network systems, and promote the implementation of innovative trust concepts to support the operation of these systems. The program should focus on articulating a vision, providing incentives for research and development, and establishing policies affecting government procurement contract awards.

This recommendation was strongly supported by telecom operators and a technology association. However it was pointed out that the complexity and costs to turn such recommendation into reality should not be underestimated suggesting that broad sponsoring by Member States would be required. Nevertheless European Institutions and Member States are not necessarily the best placed to develop and oversee the activities proposed.

Although the other contributors also agreed with the present recommendation, they considered that some risks exist. First, Internet and NIS service providers and an EU public body pointed out that if the recommendation is not designed and applied with great caution it could stifle competition in a free and competitive market and possibly put Europe in competitive disadvantage in relation to worldwide players. Second, having a monoculture in information security for instance could create a single point of failure and hence have as side effects the reduction of innovation and limitation of choice. Indeed, diversity may actually prove beneficial, since compromised trust or security with one provider would not necessarily have an impact on any other part of the supply chain.

Another respondent also suggested that an asset-oriented approach identifying asset-specific security levels and implementing proportionate security measures may be more appropriate than an overall end-to-end supply-chain integrity and trusted operation program. It also mentioned that the subject of Trusted Computing was not sufficiently addressed in the ARECI report.

A respondent pointed out the risk of single actor domination of the supply chain that can cause several problems in a crisis situation, such as not being able to meet service level agreements due to high volume of support requests or due to user's location or affiliation which might not allow support to be obtained due to economic, military or disaster reasons. Therefore, open and standardised interfaces between software and hardware components should be promoted. Likewise, the respondent underlined that the access to software source code, especially of critical communications infrastructures, would prove to be beneficial because it would enable to switch vendors, obtain fixes or updates to software from parties other than the original vendor including in-house developments.

Recommendation 7 – Unified European Voice in Standards

Member States should consider opportunities to coordinate positions during standards development, since multiple voices speaking in unison can give the European Union members more leverage in addressing concerns of mutual interest to the members. The Member States should coordinate the selection of standards bodies in which to actively participate. Member States should agree on which standards to follow to minimise conflicts.

With regard to this recommendation, only two respondents seemed to support it. One of the two contributors welcomed greater coordination of European positions concerning standardisation issues.

The other contributors did not support the recommendation as it is drafted. It was said that such recommendation is contrary to European competition rules and somehow unrealistic because there are several competing fora addressing the same technical issues. A unified EU voice in standards would make standardisation less technical and more political. In fact, while a unified EU voice may create a more simple standards framework for companies, they would still need to comply with international standards if they operate on global markets, resulting in a more complex and confusing standards

framework. Therefore, it is neither desirable to complicate the development of standards nor to close the EU market to international third parties. In addition, the establishment of a single standard does not guarantee better security and can actually create a single point of failure. Finally, it was supported that standards development should remain an industry-lead activity, but cooperation between industry and Member States would be advantageous in order to assist EU public policy aims and meet the requirements and needs of Member States .

Recommendation 8 – Interoperability Testing

The Private Sector and Member States should develop an industry-consensus, standardised, network-to-network testing framework to ensure that a rigorous set of tests are performed prior to interconnecting new networks to existing networks.

This recommendation was supported by all the contributors except two respondents. However, it was mentioned that the description of the recommendation should be more detailed in particular in terms of scope and criteria of the testing framework. Although interoperability testing is definitely needed, security aspects such as penetration and vulnerability testing and risk assessment of new networks should be emphasized.

Internet service providers were uncertain about the need for such a recommendation, since testing is obligatory from the operators' point of view and if not done properly networks do not work. A technology association also agreed with this perspective, but pointed out that interoperability testing will not find dangerous 'common-mode' failures and will not expose the unknown.

A respondent also emphasized that stakeholders acting in the regulation field should have an active role to achieve the necessary consensus in the implementation of this recommendation.

Recommendation 9 – Vigorous Ownership of Partnering Health

European Institutions, Member States and the Private Sector should re-invent their approach to collaborating and embrace a mind-set of unilateral responsibility for the success or failure of critical Public–Private Partnerships.

Although this recommendation was supported by almost all the respondents, one contributor raised the question of how this partnership will be different from what is proposed in the recommendations on information sharing and the use of industry-consensus best practices – would Public-Private Partnerships lead to decision making or would it just support the exchange of information? Generally all contributors agreed that trust between the private sector and governments should be promoted. Telecom and NIS providers also noted that the most important elements of such partnership will be: promoting equal partnership, sharing of information in a confidential and effective manner and agreeing in a common approach between all stakeholders. In line with this view, one contributor suggested the establishment of a national Critical Infrastructure Protection authority by each Member State in order to foster coordination and communication between government and industry stakeholders on key critical infrastructure issues.

Another respondent emphasized that if some new approach is needed, it should be based on voluntary cooperation that would likely be more successful than governments enforcing regulation.

Recommendation 10 – Discretionary European Expert Best Practices

European Institutions and Member States should encourage the use of discretionary, industry-consensus Best Practices to promote the availability and robustness of Europe's electronic communications networks. The Private Sector should contribute its expertise to industry Best Practice collaboration and implement the resulting Best Practices, where appropriate.

All contributors seemed to agree that sharing and using Best Practices is beneficial across the various ICT industry sectors and can serve as a useful tool or basis for further discussions. However, some respondents noted that it will take some time and will be costly to implement such a recommendation. An active intervention of governments and regulators was requested by an operator. According to an association in the field of NIS a trusted and effective information sharing infrastructure will be crucial for the success of the recommendation. This respondent actually made reference to the existing information sharing framework in the United Kingdom called Traffic Light Protocol. Internet services providers agreed with this recommendation as a way to foster the development of network security. Its implementation should however respect the unique know-how of service and network operators.

Lastly, it was noted that the study could have actually presented how European Institutions and Member States can encourage the use of best practices and which incentives can be presented to industry stakeholders.

3. ANNEX – LIST OF CONTRIBUTORS

Table 1 - List of contributors

CATV – TV Cabo Portugal	Telecom operator
Cyber Security Industry Alliance (CSIA)	Industry association (cyber security software, hardware and service companies)
Deutsche Telekom	Telecom operator; Member of ETNO
European Network and Information Security Agency (ENISA)	
EURespond	Alliance of individuals, NGOs, regions and corporations that support efforts to protect critical infrastructure
European Internet Services Providers Association (EuroISPA)	Industry association
European Telecommunications Network Operators' Association (ETNO)	Industry association
France Telecom	Telecom operator; Member of ETNO
ICP – ANACOM	Portuguese telecommunications regulatory authority
The Institution of Engineering and Technology (IET)	Professional society for the engineering and technology community
Information Society Strategy Working Group of Green League (Green League)	Political party
International Telecommunication Union (ITU)	Standardisation body
European Commission's Joint Research Centre (JRC)	
Spain Permanent Representation to the European Union (ES)	
Symantec	Security software and services provider; Member of CSIA
TerreStar Global	Mobile satellite services provider