



European Network and Information Security Agency
Science and Technology Park of Crete (ITE)
PO Box 1309
71001 Heraklion, Greece
<http://www.enisa.europa.eu/>
Tel: +30 2810 391280
Fax: +30 2810 391410

Heraklion, 3rd May, 2007

ENISA comments on the EC study on availability and robustness of electronic communication infrastructure

1 Context

ENISA received a request (see email in Annex A) to comment on a study on availability and robustness of electronic communication infrastructure. The deadline to receive comments is 18th May.

In this document, ENISA expresses its point of view on the recommendations presented in this study.

The study is available here:

http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3334

A general comment on the study is that it describes problems but does not suggest detailed solutions. ENISA agrees in general with the suggested recommendations, but would like to make the following comments. ENISA would also like to suggest two other recommendations.

2 ENISA comments

Recommendation 4.1

This recommendation is very important, and to some extent self-evident in a study on availability of critical infrastructure, because it's a central concept of all Business Continuity Management methods. It should also be noted that joint emergency exercises are just one phase in a more complete Risk Management framework that comprises a deep analysis of the system with the interconnections between subsystems, mutual dependencies and of the vulnerabilities and threats that can affect it. Performing joint exercises is a way to test and improve the risk-mitigation countermeasures put in place after that analysis.

Today's most known methods for Risk Management are not tailored to deal with large dependable systems, which cross-border and cross-organizational, and in particular with multi-level governance models.

Therefore, it could be suggested that:

- the recommendation specifically refer to business continuity/risk management approaches (including the analysis of possible scenarios and cascading effects) as a prerequisite for emergency preparedness;

- EU and Member States should also foster research on Risk Management/Risk Assessment methods to address large dependable systems, as in public communication networks. This could be a powerful driver towards more resilient interconnected systems, considering also that single enterprises alone will find it difficult to afford the cost of these analyses.
- To use the inventory of risk management methods and tools created by ENISA. See more details on: <http://www.enisa.europa.eu/rmra>

Recommendation 4.2

It would be good to differentiate between types of emergency communications. Implementing priorities on public networks is only one solution, another one being ad-hoc peer-to-peer networks (which could be considered as a way of creating public networks rather than using them). Moreover, the type of priority needed depends on the infrastructure and the emergency situation. In case of a local disaster (e.g. a bushfire), a network might have to prioritize voice calls. In case of a worm outbreak, priority might go to DNS services. In case of a stock market crash, priority might go to financial communications.

Regarding Recommendation 2: "Public networks" does not mean that they are run by the "public sector". In fact, most networks today are run by the private sector, and it is difficult to see how governments would "implement" something on these networks. Governments could, however, request or regulate priority communications on such networks.

The chapter describes that priority on future networks will be more challenging than on a legacy network. However, it can also be seen as an opportunity, because priority features can be designed into the network infrastructure from the very beginning.

It is worth referring to EU directive 2002/22 EC on universal service, in particular, article 23 of this directive which describes the recommendations regarding the integrity of the network.

Recommendation 4.3

ENISA welcomes the idea of fostering formal mutual aid agreements between industry stakeholders. Today's communication networks are complex cross-ownership and cross-border systems which require a coordinated crisis approach. Formal mutual aid agreements are a means to realise such an approach and thus constitute a way to increase interoperable crisis reaction capacities of the industry as a whole. Therefore, ENISA comments on the recommendation as follows:

- It should be noted that a formal mutual aid agreement must encompass different security levels on a network. Therefore, instead of incorporating abstract definitions of threats and vulnerabilities, it should be based on an asset oriented approach. Such an approach calls for a sound evaluation of risk and business continuity factors. The recommendation should therefore stress the fact that Member States governments, European Institutions and industry will have to gather and conduct preparatory risk and business continuity assessments in order to create focussed mutual aid agreements.
- It is clear that mutual aid agreements for critical infrastructure contain a considerable public interest perspective. Therefore, the role of Member States and European Institutions in the definition, establishment and implementation of such agreements should be underlined more clearly. In particular, Member States and European Institutions can support the introduction of mutual aid agreements by fostering relevant public research (e.g. in the area of business continuity), by setting incentives and by enabling economic operators of various sizes to participate in such agreements.

- Due to the cross-border nature of networks, any programme on the promotion of European formal mutual aid agreements should clearly focus on the European perspective. Agreement templates and their implementations should ensure a uniform application of agreed definitions and standards in all Member States and foresee specific processes for cross-border transactions in crisis situations.
- When examining regulation under their jurisdiction (Step 3-1), Member States and European Institutions should especially consider questions of scale and scope of mutual aid agreements and respective competition issues.

Recommendation 4.4

As in several other Recommendations in this report, this Recommendation is quite generic, leaving room for interpretation. Ideally, the Recommendation and its Required Commitments would be more specific, suggesting concrete measures.

Moreover, there is a major aspect missing in the discussion here – the aspect of "motivation". The "Required Commitments" (b) to (d) simply state the private sector service providers and government authorities "must be willing to share information for the common good". ENISA's experience is that this does not work. Organisations might generally be willing to share information, but in reality this does not happen (especially not with sensitive information) unless there is a very clear (mostly monetary or regulatory) incentive to do so. "Motivation" has to be added to the discussion.

Regarding "Next Steps": Although we agree that a star topology is not appropriate for reasons of trust and single-point-of-failure, we do believe that an element of European coordination is necessary. So far these "next steps" discuss information sharing only within or between member states, but do not mention how this would be coordinated in Europe.

In this respect, it may be worth noting that ENISA is working on information sharing within two projects as requested by the European Commission:

- Examining the feasibility of a data collection framework;
- Examining the feasibility of an EU-wide information sharing and alert system.

Along the same lines, a new project coordinated by Mitre could be tracked: Common Event Expression – A standard log language for event interoperability in electronic systems.

Recommendation 4.5

This recommendation is crucial to make telecommunication networks more resilient. In fact, the analysis of inter-dependencies in a complex system is a central concept of ALL Business Continuity Management methods.

However, the Recommendation as stated in 4.5 (similar to the way it is stated in 4.1) is very generic. Ideally, such an analysis of inter-dependencies would be taken in a specific context, using an agreed methodology, for example a common risk assessment or risk management methodology.

In that respect the suggestion given in point "Next Step 5.2" (a joint effort of European Institutions and Member States) is most welcome, because no single organization could afford the costs of this analysis, and public funding is an important driver to address this issue.

"Next Step 5-3" also touches on an aspect that is otherwise missing in this recommendation: understanding inter-dependencies is only a first step; providing solutions on how to deal with these inter-

dependencies is a step that has to follow immediately. This report will be the motivation for funding proposals. These future projects should not only look at the problem, but also identify possible solutions.

It can be argued whether a “reduction of inter-dependencies” is a realistic goal, given that the infrastructures supporting world-wide telecommunication networks are going to be even more interdependent in the future. If inter-dependency is interpreted as “single-point-of-failure”, then the introduction of redundancy can be a possible solution. Adding a redundant path between two critical networks indeed means that they are less dependent on each path, and inter-dependency (as single-point-of-failure) is reduced.

At a time of globalisation, consolidation of infrastructure (i.e. bigger, often more central) is a general tendency of the market. Reduction of inter-dependencies is a movement in the opposite direction. Consequently, one way of doing so might be through government regulation, i.e. by artificially limiting dependencies as it is done for example in the area of large enterprise mergers.

Recommendation 4.6

ENISA agrees to the notion that managing and securing the network elements of future ICT networks will constitute an increasingly challenging task. In order to succeed in this task, a coordinated approach between Member States, European Institutions and industry will be necessary. The study rightly points out that supply chain integrity management and trusted operation concepts for network elements are powerful tools for network security management in future networks. If such tools are implemented following a uniform end-to-end security concept agreed between Member States, European Institutions and industry, they allow for extensive control to be executed over virtually all network elements, including end-user infrastructure.

However, such an approach may not properly take into account different security levels on a network. As the study rightly points out, governments may have a security level calling for closed supply chains and trusted environments. The same may not be true though for other players on the network, such as small or medium sized ISPs. Therefore, 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 regime. For many sectors of Internet and other public telecommunication networks, having Member States and EU pushing to take into account the best standards in terms of security and confidentiality could be a more proper recommendation, whereas trusted computing could be considered as a too strong instrument. A suggestion related to standards is absent in this recommendation.

In this context, it should be pointed out that the study does not sufficiently refer to the public discussion currently taking place on the subject of Trusted Computing. In particular it does not evaluate stakeholder contributions¹ claiming that trusted operation regimes and trusted computing in particular do not deliver appropriate security levels and may have a negative effect on ICT markets. Stakeholders claim that trusted computing may slow down ICT growth by hampering product innovation cycles and impeding innovation in certain market areas such as FLOSS².

ICT remains a major factor in driving growth and innovation.³ Moreover, FLOSS market share is particularly high in the EU and there is an increasing number of globally successful European SMEs

¹ See for example the Free Software Foundation (www.fsf.org).

² Free/Libre/Open Source Software.

³ European Commission, Communication "i2010 - Annual Information Society Report 2007, COM(2007)146 final.

specialising in the sector.⁴ FLOSS can make Europe a technology leader⁵, and for this reason EU should pay a special attention to the debate on Trusted Computing, which could limit its development if applied in a pervasive way. Therefore, the study should evaluate the current public discussion in order to assess whether an asset-based approach, taking into account specific security levels is preferable to overall supply chain integrity and trusted operation management.

It should also be noted that the debate on Trusted Computing is closely correlated to the debate on Digital Rights Management (DRM), because trusted computing is considered as one of the best technical solutions to support DRM.

Recommendation 4.7

The chapter strongly stresses the need for a direct participation of Member States in standardisation. ENISA does not think this is the most efficient and successful way to go, as we think industry remains the leading driver of standardisation. It can be argued that it depends on the particular standardisation body, for example the ITU uses country-representation and they have representatives of the MS (e.g. from the ministry) alongside industry. But as far as we know, for a body like the IETF, which is the one mentioned in the chapter, the channel to go through is industry.

ENISA thinks the main stress should be put on the need for an effort to set up cooperation between industry and Member States (e.g. in the matter of preparatory activities, requirements, planning, gap analysis) and to support the development of standards that can meet the requirements and needs of Member States and other costumers, remembering that these requirements and needs are continuously evolving and changing.

Further stress should be put on the need for information sharing and for involvement of all stakeholders in all the steps of pre-standardisation and standardisation – starting from the requirements-capture phase.

More comments:

- Paragraph 3: there are other issues, e.g. fragmentation of standards, and often the presence of a number of solutions while none emerges as a commonly accepted standard (in this case it is difficult to understand which solution to implement).
- Paragraph 3: 'MS may have a vested interest in national companies...' We cannot judge if this is true so we would expect to see is a source for this statement? (We have not seen it in our standardization experience, but CIIP could be different case)
- Paragraph 4: see our general comment above. It is true that IETF is individual based but that companies are behind it, in fact to make a standard progress in IETF (as in other SDOs in general) there is the need of their support. Successful participation in standardisation requires the right involvement and the right support, hence ENISA sees a stress on the need for effort of cooperation of Member States with industry, with industry as driver as more fruitful, rather than stressing 'direct participation' of MS,.
- Recommendation 7: see our general comment above. Rather than 'direct participation', we would recommend the effort to cooperate with industry by e.g. elaborating the right requirements, creating a forum for discussion and information sharing where all the stakeholders are involved supporting actions and incentives.

⁴ Study on the Economic impact of open source software on innovation and competitiveness of the Information and Communication Technologies sector in the EU, UNU-MERIT (<http://ec.europa.eu/enterprise/ict/policy/doc/2006-11-20-flossimpact.pdf>).

⁵ <http://istresults.cordis.europa.eu/index.cfm/section/news/tpl/article/BrowsingType/Features/ID/80607>.

- Next steps:
 - 7.1. ENISA is not sure what are the 'standards bodies requirements' to be 'followed'. We believe the way to go is to work with industry to develop such requirements and then get them into standardisation (through industry).
 - 7.2 ENISA thinks a step back is needed. Member States can work to set requirements, together with industry. A forum could be created to facilitate discussion and cooperation. Then the industry would take care of the standardisation process. Appropriate incentives need to be found. Also, support is needed for development and implementation of standards so that they can become commonly accepted.
- Measure of success. In our opinion, uniformity of standards is less important than interoperability.

Recommendation 4.8

This recommendation is too general. The substantial content of this section could be condensed the following statement: "There is a need to test interoperability between different branches of a networked system to guarantee robustness. This should be standardised in an industry-wide standard which is also endorsed by the Commission and MS".

We feel that although this is reasonable, it does not give enough detail. For example the following are missing:

- What are the conditions to trigger testing? What is a "new network", or indeed a network in this context is not clear enough? Does this refer to connection of LANs under different ownership, new technologies such as IPV6-IPV4? ... The document's terminology section does not clarify this.
- What kind of testing is envisaged - Automated, Audit-based?
- Are there best-practices on which the standard could be based?
- How should the open governance of such an important standard be guaranteed?

In the suggested idea of an interoperability testing framework developed by "the industry as a whole", and endorsed by Member States and European Union, special attention has to be paid to the presence of SMEs in any context in which the framework is going to be discussed. This is important to avoid the risk of affecting the market in the European economy, with its strong presence of SME's, and to guarantee the impartiality needed to make this important idea successful.

Recommendation 4.9

Although ENISA completely agrees with the content of this Recommendation, the wording is unfortunate. In a discussion on critical infrastructures where the "health sector" itself is often seen as a critical infrastructure, having "Partnering Health" in the title is confusing. Instead, the well-established term "public-private partnership" should be used. So the title would be "Responsible Ownership in Public-Private Partnerships".

Moreover, like Recommendation 4.3 does not address the motivation of partners to work together. Telling partners that they "must" do something is not enough; explaining to them "why" it is necessary and especially "how" they would benefit from that partnership is crucial.

Recommendation 4.10

ENISA completely supports the recommendation to use and promote industry-consensus best practices. However, implementing them will take time and involve costs (staff training, dedicated resources, software/hardware...), the study could have presented incentive for Service Providers and Network Operators to adopt and implement them.

The development and implementation of Best Practices will be mainly supported by industry. No details are given of how European Institutions and Member States should encourage the use of best practices. This could be clarified.

ENISA suggests that the European Institutions foster research and studies on discussion mechanisms between stakeholders to create Best Practices.

3 Others possible recommendations

ENISA would like to suggest other areas where recommendations could help:

- There is a lack of methodology on Risk Analysis, interdependency, Business Continuity, cascading effect and certification for large infrastructure. This lack of methodology could be taken in account within FP7 projects selection.
- Governance of e-communication systems could be taken in account during the revision process of the telecoms package⁶.

4 Key findings

Generic comment

The criteria for assigning an observation to one Maturity Level are not very clear. For example, observation 80 on page 82: this issue might be resolved via asset management together with a method to evaluate impacts on ITC-configurations (see comment 2 below). For both solution alternatives, no current standards exist, so this observation could be part of Maturity Level 5. Same goes for observations 65, 78 and 81, among others.

It should be noted that the observations made are mainly technology oriented. Besides that, organizational issues are also of profound importance for the implementation of security. Such organisational issues seem not to be the main focus of this report (at least what the observations is concerning).

Comments on observations from Maturity Level 4 (55-83) and 5 (84-100)

The following key issues from the security point of view are not mentioned in the study. They seem to be of fundamental importance for the availability and robustness of infrastructures.

1. Security Level of involved entities: It has to be mentioned, that entities involved in the service provision of telecommunications are of different security levels, ranging from none (e.g. multiple end-users, small ISPs) to very high-level (e.g. big telecommunication companies). Possible security gaps between players in the supply chain lead to various security problems. This relates to (or is the reason for) observations: 61, 66, 71, 73 and 76.

2. Security should be expressed on the basis of assets: In order to find appropriate security levels needed within a network, an asset-oriented approach should be adopted. Security will be expressed according to the risk-level of this asset. This relates to (or is the reason for) observations: 64, 72 and 80.

3. Enforcement of security for all assets involved in telecommunication service provision: Irrespective whether the life-cycle of assets is in-sourced or out-sourced (development, test, operations), the security level assigned to this asset depends on the sensitivity of the data it processes and it should be homogeneously enforced throughout the entire life-cycle. This usually leads to the adoption of Risk

⁶ The telecom package refers to EU directives 2002/19/EC, 2002/20/EC, 2002/21/EC and 2002/22/EC.

Management/Risk Assessment for the involved assets. This relates to (or is the reason for) observations: 58, 62, 66, 76 and 77.

4. *Future networks will integrate simple devices with very low or no security:* Ambient Intelligence and the *internet-of-things* are going to lead to configurations where security is not part of simplified devices assigned e.g. to sensors. The *internet-of-things* will give opportunities for new attack scenarios that will be easy to run against unprotected network assets.

5. *Absence of a model to express threat level of a component:* For the time being, there is no possibility to express how an identified threat can affect a certain infrastructure component depending on the context of its use (e.g. degree of dependency on other components, criticality of its use etc.). This relates to (or is the reason for) observations: 80 and 99.

6. *Establishment of a managed and controlled security framework:* Security should undergo permanent improvement based on detected incidents. This includes the implementation of network controls for this purpose (dynamic and static, automated or manual). The management and control of the network and its assets should be implemented in a secure way. This relates to (or is the reason for) observations: 65, 95 and 96.

Annex A

Request received by email.

From: Leo.Koolen@ec.europa.eu [mailto:Leo.Koolen@ec.europa.eu]

Sent: 02 April 2007 17:39

To: Leo.Koolen@ec.europa.eu

Subject: Call for comments on the report of a study on the availability and robustness of electronic communication networks

Dear colleague,

Alcatel-Lucent Technologies carried out a study for the European Commission on the availability and robustness of electronic communication networks. The study provides insights in the availability and robustness of electronic communication networks and makes a number of key recommendations to enhance their protection and resilience. The final report of the study is now available on http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3334

The Commission seeks comments on this report from all parties that may have an interest. As the report will be an important input for establishing an agenda for a multi-stakeholder dialogue on this matter in Europe, we are particularly interested in any views you may have including on its scope, the approach and orientations taken, the issues addressed etc. But of course also detailed comments on findings and recommendations as well as the technical annexes are welcome. The deadline from comments has been extended until 18 May 2007. Further details can be found on the above weblink.

If you represent an organisation or association, I would much appreciate it if you could circulate this message among those members of your organisation or association that may have an interest in this matter. Thank you very much in advance.

Best regards,

Leo Koolen