



June 2007

EuroISPA comments on the study on the availability and robustness of electronic communication networks

EuroISPA is the world's largest association of Internet Service Providers, representing approximately 1000 ISPs across the EU. Our industry comprises many stakeholders in the area of network security, some of whom are actively involved in initiatives at Member State level, as well as in discussions and technical development in the international arena. Our members are therefore following the European Commission's work in this area with great interest.

Introduction

EuroISPA thanks the Commission for the opportunity to comment on this study. Our members recognise that this piece of work will contribute to the Commission's initiatives in the areas of general network security and critical infrastructure protection. We therefore appreciate the Commission's efforts to actively promote the study and urge relevant stakeholders to submit their comments for the Commission's, and other interested parties' consideration.

Overall Remarks

The study team has undertaken a significant piece of work in an area that contains many issues that will receive ongoing attention in the coming years. There is much in the study with which EuroISPA agrees – therefore, given the scale of the study, we believe it is most useful for us to concentrate our remarks on those aspects of the document with which we either do not agree or would like to see clarified.

The following remarks concentrate on general issues in relation to the study. These relate to the terminology and some aspects of the study methodology.

EuroISPA believes the authors' notion of a **maturity model** was an excellent basis for the study. However, it is rather unclear to our members on which practical criteria the maturity model is based: we believe it would have been advantageous to specify whether, or to what extent, this referred to issues such as maturity in the implementation of new technologies, best-practice, risk management or cooperation with other stakeholders, for example. In addition, whilst there will be always be overlaps between the specified levels, we think some inconsistencies could have been avoided.

The term “**robustness**” is something that is not widely used among Internet service providers and therefore we have some difficulty understanding its application within this piece of work. We note the study authors have given the term a very detailed definition, but it seems that on this basis, the terms “availability” and “robustness” appear to equate with “business contingency” and “continuity planning”. EuroISPA believes it is unhelpful to highlight new terminology without any specific reason. In any case, the study actually says very little about “robustness”, which may be the consequence of this.

EuroISPA fully agrees with Study Finding 54, which says there are **too many studies, initiatives, reports and recommendations**. This is the fault of all stakeholders and we accept the study team’s assertion that this leads to too many valuable resources being expended in projects of limited use. EuroISPA proposes that this study could give rise to a discussion at the next workshop on how industry as a whole could better manage this area, in conjunction with other stakeholders.

Whilst we appreciate the difficulty in combining assessment of the traditional communications world with more recently introduced or established technologies, EuroISPA believes the study recommendations and findings are **more past-related than future orientated**. The study team has included an excellent, extensive and comprehensive list of technologies in the annexes to this study, but these do not seem to have had a major impact on the study’s findings and recommendations. Indeed, some of the terminology used (such as “calls”, “priority calls”, “incumbents” and “new entrants”), whilst still reflecting the main terms used in many EU Member States, does not reflect a future-orientated perspective of the issues. Again, we do not intend this to be a particular criticism of the study, since the study team may have reasonably decided that the use of such terminology would make the study more accessible for most stakeholders: however, we do believe this is a useful observation and could be a starting point for discussions on how we assess some of the study’s recommendations in the context of new technologies. EuroISPA would also repeat this observation in relation to Section 2.4.4 (Other aspects of Representation), where the terms used are incumbents, new entrants and non-profit organizations¹.

Study Introduction (Section 2)

In section 2.2.1., the study lists eight items that make up the ingredients of a communications infrastructure. EuroISPA believes these eight ingredients would be perfectly adequate if the scope of this study would only be the critical network infrastructure. However, this study also examines additional levels, in other sectors, around critical infrastructure. For example, we believe the payload is more related to other sectors than the network itself in the context of this study (see figure 2, p. 23).

Section 2.4.1. – the “Private Sector” – lists industry roles in the communications industry. The study correctly notes that the term “service provider” incorporates a huge variety of stakeholders, each with very different roles – such as access providers and hosting service providers. Unfortunately, detailed further assessment of the different roles of different “service providers” clearly extend well beyond the scope of

¹ We do not believe that it is helpful to categorize companies this way anymore, especially when referring to technical issues, because incumbents are also new entrants in some areas, new entrants may carry some part of their business as incumbents and non-profit organizations may be active in areas usually thought of as belonging to incumbents or entrants.

this study, but EuroISPA urges policy makers to take note of this point, as it is integral to the development of appropriate, well-targeted initiatives in relation to network security.

Study Key Findings

In this section, EuroISPA outlines its observations on a number of the study's key findings.

Maturity Level 1

Finding 4: Future network operators may not be recognized as part of the critical infrastructure

EuroISPA would like to note that future network operators will not necessarily be operators of critical infrastructure. The issue of which network operators are operating “critical infrastructure” is something that will doubtless be discussed within the context of the European Commission's specific policy initiatives in this area, to which this study contributes valuable information. For now, it is sufficient to note that “criticality” means that a critical operator has to have critical services or customers of “critical-labelled” services connected to their network.

Finding 5: Government engages network operators too late.

We fully agree with the study team's finding on this point. It is clear that the private sector produces network availability and “robustness”, not the public sector itself. There are signs that governments are starting to engage more proactively with industry on these important issues, but we would welcome a further discussion on best-practice in this area.

Maturity Level 2

Finding 6: The deployment of priority services is awaiting government funding

EuroISPA sympathises with this finding, but also notes that priority communication services are not merely a question of funding. For example, there is no common currently available technology in use to implement prioritized interconnection traffic between packet switched networks. Therefore, we do not believe this is a government funding issue, aside of course from government-sponsored research and development projects.

Finding 7: Multiple standards bodies are producing different standards

To supplement the finding, EuroISPA would add two remarks. In addition to those bodies mentioned, there are more than 400 forums producing *de facto* standards. Also, standards usually include several options, so even using the same standard does not always guarantee interoperability.

Finding 11: High costs associated with security and availability

EuroISPA very much agrees with the main sentiments set out in this finding. However, we do not necessarily share the view that, “Newer applications will tend to be initially deployed with lower reliability levels.” Newer applications are not usually critical at the moment of birth.

Finding 12: Reliability and security are challenged by the migration to future networks

EuroISPA does not believe the basis for this finding to be necessarily valid. If the reliability and security of an emerging network is poor, there will simply be no commercial boost for that network. Our members stress that there is a market driven need for reliability and security. Therefore, the migration to future networks should be seen as an opportunity, rather than a threat.

Finding 18: The level of emergency preparedness varies greatly across Europe

EuroISPA believes it is useful to add to this finding that the level of emergency preparedness varies greatly not just across Europe, but within each Member State and across critical infrastructure operators in each Member State.

It is also useful to note that there may be some natural overlap between business continuity management plans and so-called “emergency preparedness”. Some Member States or operators in some Member States may have not put emergency preparedness plans in place, but they might have advanced business continuity management plans that would serve the same purpose.

Finding 21: Collaboration between governments and the private sector needs improvement

EuroISPA would support this general remark and suggest further discussions on how best to address this issue.

Finding 22: Quality, reliability, and security will vary greatly in future networks

EuroISPA understands the basis for this finding, but we believe it does not sufficiently reflect the needs of the market. There is no demand for poor quality, reliability and security!

Maturity Level 3

Finding 29: Priority restoration for critical subscribers is not commonly supported

EuroISPA agrees with the study team’s finding, but wishes to note the complexity of this topic. We would suggest that market driven service level agreements (SLAs) are a must in an open market and that regulatory burdens on some of the market players is not an appropriate solution.

Finding 30: Interconnection testing is not based on a recognized standards-based framework

EuroISPA finds that the lack of consideration of the role of Internet exchanges is an important omission that impacts this finding. Internet exchange points will play a significant role in interconnections in the

future, which has been completely bypassed in the study. Exchanges have their own rules of how to connect to a certain exchange point.

Another issue that might be worthy of consideration is that placing barriers to interconnection on the basis of security might also be a way to prevent competitors' access to a network. The Commission and national regulators should be wary of this possibility.

Finding 33: Time-to-market pressure influences reliability and security

EuroISPA refers to its comments on other findings: whilst we can understand this finding, there is certainly a market driven need for reliability and security, without which the stakeholder concerned will be out of business!

Finding 39: Future networks will be more difficult to manage

EuroISPA is unsure whether this finding is correct – some of our members believe future networks might be more inherently resilient and therefore require less human management (i.e. increased efficiency in this regard). We would welcome further detail and discussion on this important statement.

Finding 41: Local governments play a key role in maintaining the reliability and security of networks

EuroISPA does not agree with this sweeping statement. A lack of security in end-users' networks does not compromise the security of publicly available networks. More important is to examine which types of connections operators offer to their customers (for example, do they provide "layer 3" (Ethernet) access?). Therefore, governments' networks may be part of critical infrastructure, but not for the reasons presented here. They might be critical due to the fact that government services in question may be vital for society.

Maturity Level 4

Finding 66: Outsourcing of hardware and software development is viewed as a risk

EuroISPA believes this sweeping statement is unhelpful. Any "risk" clearly needs to be associated with the criticality of the task that has been outsourced. Indeed it could even be argued that the risks are much smaller in comparison with the situation prior to outsourcing. Therefore, we would favour assurance mechanisms that provide confidence in hardware and software development lifecycles, regardless of whether they are outsourced or not.

Finding 67: (footer 75) 77% of subject matter experts confirm that open source software negatively impacts reliability and security

EuroISPA notes this point and believes it would be a useful further discussion item. Our members do not believe open source is a reason in itself for a lack of reliability and security – clearly if software quality is low, whether it is open source or not is irrelevant.

Finding 72: Protecting networks from misuse requires comprehensive security design

EuroISPA believes this finding would benefit from more detail, in order to better define network misuse and distinguish this from service misuse. The examples currently used involve content carried by the network and its elements.

Finding 73: End-user's awareness of security issues and end-device security setting is lacking

EuroISPA agrees that this is clearly a significant issue and echoes the study team's assertion that some stakeholders have public awareness campaigns in place. The Commission has been a strong advocate of such initiatives. In addition, EuroISPA notes that there is a need for systems to be designed and built securely enough for normal use without end-user participation in the security management of their device.

Finding 74: Federated Identity Management will become a compelling security strategy in future networks

EuroISPA is unsure whether this statement is correct. We believe identity management and compatible authentication systems will certainly be "a must" and are compelling, but we do not agree that federated identity management necessarily will be. Service-matched identity management and authentication will be very important, but "one-size-fits-all" thinking is not realistic.

The key is less that we have a federated (the term "federated ID management can and has been defined in different ways by different actors) scheme but rather that we have an interoperable one with an overarching identity metasystem with sufficient levels of assurance. What is important is the development of trust – in third parties, not only on technological issues.

Finding 75: Future networks are more vulnerable to signalling fraud from end-user devices

EuroISPA wishes to reiterate that we must make a conscious distinction between network signalling and service misuse whenever possible. This finding is not about fraud (which indicates an attempt at some form of unlawful financial gain), it is about something else, such as spoof signalling or network (management) control messages.

Finding 77: New equipment vendors may have an adverse impact on the supply chain

EuroISPA doesn't believe the inference in this finding is helpful. "New" is not a synonym for "bad", while whether something is "new" is dependent on other circumstances (e.g. new to us, new to the market, an entirely new entrant to the vendor market?).

Finding 82: Sessions traversing diverse networks result in various degrees of QoS

EuroISPA agrees that the issue of prioritised traffic is important. Given the importance that is seemingly attached to this subject, since it is mentioned in various places in the study, we would have welcomed a specific section examining the issue of service level agreements, which incorporate quality of service criteria.

Maturity Level 5

Finding 84: Disaster recovery arrangements across national boundaries are limited

EuroISPA is unsure whether the impact of such lack of coordination between Member States is theoretical or if there is further evidence to suggest severe practical issues. In any case, EuroISPA assumes that this will be a major point of discussion with all stakeholders in the European Commission's development of its programme for Critical Infrastructure Protection.

Finding 86: Priority communications mechanisms are needed between member states

The scope of this finding and consequently the outlined requirement is unclear to EuroISPA. It would be useful to have an understanding of which calls or communications (which are in themselves different concepts) authorities might need to make between each other.

Finding 88: The European Union Member States do not have unified influence on communications standards

This is an important finding, which EuroISPA addresses in greater detail in our remarks on Recommendation 7.

Finding 95: Future networks co-mingle control messages with normal subscriber traffic

Consistent with several of our other remarks on the study findings, EuroISPA asks whether this is a risk for the networks or for services.

Finding 97: Reliability and security practices vary considerably across network operators and service providers

EuroISPA very much agrees that the exchange of best-practice is to be encouraged. However, we would point out the exchange of best-practice should not be equated with common practices by all stakeholders. This would likely actually increase vulnerabilities, because diversity in approaches to network security helps to reduce the likelihood of common risks.

Study Recommendations

The study's ten recommendations are based on the 100 key findings. EuroISPA's comments concentrate on the main aspects of each recommendation.

Recommendation 1: Emergency Preparedness

EuroISPA is unsure to what extent emergency exercises and priority restoration exercises contribute to the enhancement of “robustness”. We would content that emergency preparedness is business continuity planning and that private sector actors should be encouraged to develop such plans accordingly.

This confusion follows into the recommended next steps. To which critical services do these points refer – communications infrastructures or other critical sectors?

Recommendation 2: Priority Communications on Public Networks

EuroISPA strongly believes this recommendation should make a distinction between circuit switched and packet switched networks. The challenges regarding prioritization are totally different in these two types of networks.

However, we would also like to point out an observation that follows from Key Finding 85, which states that “Several Member States have separate communications networks for critical functions. In other Member States, this is not the case and private and public networks are not physically separate. 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. This doesn’t seem to have been fully considered in the study.

Recommendation 3: Formal Mutual Aid Agreements

EuroISPA believes this Recommendation is likely to be a good idea. However, we warn that this recommendation will be difficult to bring to fruition, since there are many issues that stakeholders cannot agree upon in relation to such issues.

Recommendation 4: Critical Infrastructure Information Sharing

EuroISPA believes this would certainly help stakeholders within the lower maturity levels described by the study team. From our perspective it is difficult to foresee how higher maturity level stakeholders would be motivated to contribute to such sharing that would focus on the stakeholders in the lower maturity levels.

Recommendation 5: Inter-Infrastructure Dependencies

EuroISPA understands the potential value of the program that the study team recommends be established. However, we think this recommendation could be improved. The outcome of the proposed analysis of dependencies is that everything is dependent on everything else. The ICT sector provides critical information for services for other sectors which cannot function without electronic and integrated information.

Being able to provide essential information and communications services is a question of business continuity planning within the ICT sector. It is recognised by EuroISPA and most other stakeholders that the value of end-users being to transmit electronic information globally when they release it onto electronic communications networks is a true dividend from the information society. From the perspective

of service providers, ensuring their customers can take advantage of this expected facility is part of business continuity planning. We therefore believe the discussion should most appropriately be focused on this concept.

Recommendation 6: Supply Chain Integrity and Trusted Operation

EuroISPA agrees with the emphasis on trust, but believes the recommendation would benefit from some clarifications. For example, does this recommendation refer to issues like Common Criteria? If so, this recommendation could lead to a quite different outcome than that which is expected. Indeed, stakeholders must also consider that rich diversity may prove beneficial, as compromised trust or security with one provider would not necessarily affect any other part of the supply chain.

Recommendation 7: Unified European Voice in Standards

EuroISPA believes this recommendation must be treated with great caution.

Firstly, we think this is an unrealistic recommendation. There are about 400 forums working on different issues, complementing the work of five to eight official standardization bodies. In reality, it's the forums in the ISP sector that create many of the de facto standards. Recommendation 7-1, that, "Member States and Private Sector service providers, network operators and equipment suppliers should establish consensus mechanisms to agree on which standards bodies requirements will be followed," is seemingly impossible, whilst there would be questions about whether this would be possible in a free and competitive market. The proof that this would be unrealistic is that there are several competing forums addressing the same technical issues.

However, there is certainly scope to focus work on obtaining a unified EU voice in some areas where this would assist agreed EU public policy aims. This would seem to be advantageous in relation to some functions, rather than technologies: for example, priority schemes or lawful interception arrangements.

Finally, EuroISPA would also be concerned at the purpose of a unified EU voice in standards. We would be especially concerned that this would make standardisation less technical and more political, which should be immediately countered.

Recommendation 8: Interoperability Testing

EuroISPA is unsure to what extent this recommendation is necessary. Testing has to be done anyway – put simply, if it is not done properly, networks don't work. "Testing" is therefore obligatory from the operators' point of view. EuroISPA points out that Internet exchange points probably have the required mechanisms for this already in place.

Recommendation 9: Vigorous Ownership of Partnering Health

EuroISPA believes this is a highly important recommendation. It is indisputable that private sector companies should foster trust with government regulators (and vice versa!).

Recommendation 10: Discretionary European Expert Best Practices

EuroISPA fully agrees with this recommendation as a way to foster the development of network security. The different "maturity models" in different EU Member States (in relation to their markets, the introduced technologies) are likely to determine whether this recommendation will be accepted or not, whilst there are likely to be some issues with motivating "early adapters" to cast away their competitive edge for the benefits of others. However, this recommendation should be supported by all stakeholders, since it has shown to be an extremely beneficial method of ensuring good practice across the various sectors of the ICT industry.

Conclusions

EuroISPA welcomes this study and believes the authors have raised a range of important issues that warrant further discussion. Given the number of stakeholders and their different perspectives on this subject, it is unsurprising that there are aspects of the study with which EuroISPA is either uncomfortable or believes could be better addressed using existing, more familiar terminology or background information. We are therefore thankful to the Commission for holding this consultation and promoting the possibility for discussions on this piece of work. Finally, we look forward to further discussing our comments with the Commission, study team and other stakeholders, in the course of meetings on this and related subjects in the coming months.

About EuroISPA:

EuroISPA is the world's largest association of Internet Service Providers, representing approximately 1000 ISPs across the EU. EuroISPA is a major voice of the Internet industry on information society subjects such as cybercrime, data protection, e-commerce regulation, EU telecommunications law and safe use of the Internet. Its secretariat is located in Brussels. EuroISPA is predominantly funded by its member and associate member associations and the members of the EuroISPA Industry Forum.

For further information on this and other matters concerning EuroISPA, please contact Richard Nash, Regulatory Affairs Manager and Secretary General, at the address set out below.