European Commission
Information Society and Media Directorate-General

AVAILABILITY AND ROBUSTNESS OF ELECTRONIC COMMUNICATIONS INFRASTRUCTURES

"The ARECI Study"

Final Report

March 2007

The opinions expressed in this Study are those of the authors and do not necessarily reflect the views of the European Commission.

This page is intentionally left blank

Prepared by:

Bell Labs and Professional Services

Alcatel·Lucent

This page is intentionally left blank

Preface

This Study submits ten bold Recommendations to European Institutions, Member States and the Private Sector for the purpose of promoting the availability and robustness of Europe's communications networks. The Recommendations are ***effective****,* ***achievable****, and* ***urgent****.*

The urgency is driven by the vital role that communications networks play in Europe's economy, society and security. Without reliable communications networks and services, public welfare is endangered, economic stability is at risk, other critical sectors are exposed, and nation-state security is threatened. The implementation of this report's Recommendations will significantly reduce these and other risks.

The implementation of these Recommendations is achievable, yet challenging. Each will require skill, resolve and genuine partnership among government entities and the Private Sector. Acceptance of this challenge was demonstrated by stakeholders' overwhelming support for the recommendations during the European Commission hosted ARECI Study Public Forum, and by a number of the Private Sector stakeholders volunteering to work on moving the implementation of several recommendations forward. For each Recommendation, this Final Report presents a background, a discussion of alternative approaches and their consequences, next steps to continue the momentum that has been established during the Study, and measures of success to gauge progress in supporting the guidance

Supporting the ten recommendations, the Study documents 100 Key Findings. In addition, a major milestone accomplished during this Study was the confirmation of 71 European Best Practices for network reliability. In order to provide more information and updates on follow-up related to the ARECI Study, the web site www.bell-labs.com/ARECI *has been established.*

Europe's future communications networks promise to usher in a new world of business and lifestyle-enhancing capabilities. Many of the benefits have not yet even been imagined. The people of Europe stand to greatly benefit from the anticipated economic efficiency, citizen connectivity, functional flexibility, and speed. This Study strongly urges European Institutions, Member States and Private Sector stakeholders to chart and embark on a new course of policy and practice that demonstrably supports highly available and highly robust communications infrastructure.

Karl F. Rauscher

KARL F. RAUSCHER
Bell Labs Lead, ARECI Study Team
Executive Director, Bell Labs Network Reliability & Security Office, Alcatel-Lucent
Founder & President, Wireless Emergency Response Team
Chair, Advisory Board, IEEE Communications Society Technical Committee on Communications Quality & Reliability

This page is intentionally left blank

Table of Contents

Table of Figures

Table of Tables

This page is intentionally left blank

1 EXECUTIVE SUMMARY

The Study on Availability and Robustness of Electronic Communications Infrastructures (ARECI) was conducted for the European Commission. This Final Report of the ARECI Study presents ten Recommendations to European Institutions, Member States and Private Sector stakeholders. These Recommendations, if implemented, will significantly enhance the availability and robustness of Europe's communications networks. This guidance is based on European stakeholder perspectives, technical policy development experience, expertise in emerging technologies and the insights captured in 100 Key Findings. Summary statistics of the ARECI Study are as follows:

10	**Recommendations** **(Section 4)**
25	**Member expert team conducted study** **(Section 7)**
71	**European-confirmed Best Practices** **(Section 2)**
81	**Intrinsic vulnerabilities considered** **(Annex B)**
100	**Key Findings** **(Section 3)**
200+	**Contributing European stakeholder experts** **(Section 2)**
300+	**Critical trends considered for impact**
30,000+	**Distinct data points researched and analyzed during study**

As Europe builds its communications infrastructure of the future, it faces enormous *technological*, *economic* and *political* challenges. A sweeping *technological* transformation is underway as many of the underlying design principles of legacy networks are being replaced with Internet Protocol (IP)-based architectures that promise a vast array of new features for consumers. *Economic* challenges include supporting both ends of the user spectrum: delivering high capacity and cutting edge features to the most flourishing business environments *while also* extending basic voice and first time Internet access to yet-to-be connected citizens. The liberalisation of markets requires successfully navigating the path of increased privatisation in such a way that encourages substantial and continued Private Sector investment and also promotes competition to protect consumers. *Political* challenges include integrating a global security environment that intensifies operational and control aspects of infrastructure with the vital interest of each European Union (EU) Member State to protect its own national security.

For Europe *to simply keep pace* with the accelerating advances of the global communications theatre, it must meet these challenges. However, for Europe to *ensure highly available* and *highly robust* communications networks, it must do more. The ten Recommendations presented in this report prescribe critical areas that should receive priority attention to achieve this objective. Because many of these issues are common across many stakeholders, **cooperation at the European level** is a repeated theme throughout this report.

Guiding Principles of Study

Several principles guided the approach taken in this Study. First, the **interests of the citizens of Europe** were in the forefront. For this reason, there is an emphasis on lifeline and emergency public safety communications.

Second, the Study was to be **forward-looking in terms of technology considerations**. Therefore, the Study factored in numerous trends, such as the increasing presence of wireless interfaces, the shift of network control from being "silicon"-based (hardware) to being software-based, the emerging capability to provision bandwidth dynamically, and the disappearance of national network boundaries as a result of global interconnectivity.

Another principle was to uphold a **European focus, yet maintain global awareness**. For this reason some issues dealing with the subject of availability and robustness are discussed in general terms as background to draw more attention to issues with specific relevance to the European stage. At the same time, the team conducting this Study integrated lessons learned from other regions of the world – in particular the United States of America - from events such as the Great Hinsdale Fire of 1988, the September 11, 2001 Terrorist Attacks, the 2003 Northeast Power Blackout and the 2005 Hurricane Katrina flooding of New Orleans.

Including all European insights that were offered was another principle on which the Study was based. This was accomplished throughout the methodology described below by seeking, and then carefully considering, input received from extensive outreach conducted via diverse means. These means included one-on-one interviews, electronic virtual surveys, multi-party interactive experts workshops, review of suggested references and research of publicly available materials.

Yet another principle was to ensure **rich representation of industry, academic and government perspectives**, with care to include both long established companies as well as new entrants. Thus, all sorts of service providers, network operators and equipment suppliers were engaged. Government perspectives were gleaned from both regulator and stakeholder agencies. The Study also obtained input from other critical sectors that depend on the communications sector.

Finally, the approach utilised **world-class proficiency in both the technical subject matter and broader policy areas** to ensure the resulting guidance would be both realistic and achievable. The core Study team consisted of individuals experienced in technical policy development, with high implementation rates of their recommendations being a matter of public record. The subject matter expertise of these individuals includes subject areas central to this Study: network reliability and security, infrastructure protection, nation-state security, emergency preparedness, disaster recovery, emergency communications, ad hoc emergency networks, hardware and software quality and government-industry collaboration. The experience base, while highly correlated with U.S. context, is international in scope and has served in advisory capacities for the design and operation of several major European networks.

Methodology of Study

The methodology used in this Study was designed to support data gathering, validation and analysis with the aim of developing meaningful guidance. There are several distinguishing characteristics of the Study's methodology. First, the Study employed a **framework of the complete list of ingredients that make up communications infrastructure**: power, environment, hardware, software, payload, network, human and policy. The striking advantage of using this framework is that it readily lends itself to the comprehensive listing of intrinsic vulnerabilities, which are *finite* – unlike threats, which, for practical purposes, are *infinite*. Present-day security approaches are for the most part founded on the threat side of the equation, which is derived from historic experience and gathered intelligence. In contrast, the intrinsic vulnerability approach, rooted in a detailed knowledge of the ingredients that make up a communications network, permits profoundly higher degrees of confidence in terms of ensuring reliability and robustness. This focus on vulnerability analysis does not exclude the use of threat analysis, which draws extensively on observed trends and the subjective perspectives of individuals. Rather, it uses that knowledge and supplements it with expert knowledge about the systems that make up communications networks.

Secondly, the Study was **heavily dependent on the expertise and experience** of both the experts who provided their perspective and the Study team that analyzed that input. The opinions of experts from all facets of the communications industry were sought as described above. Thousands of years of experience are represented in the data that the team analyzed. It is worth noting that the dimension of experience that was drawn upon is not solely restricted to years of experience, but breathe of experience as well. Experts with limited years in the industry but with new and unique perspectives were included in the Study. Future networks will be a collection of a diverse set of components – analyzing them requires a diverse set of perspectives.

Next, the findings of the Study were strongly influenced by the **face-to-face interaction**. Interviews were not question and answer sessions but a two-way flow of information, with experts on both sides of the table building on and learning from each other's thoughts and ideas. The four experts workshops were the culmination of this interaction. Focusing on specific ingredients of the communications infrastructure, each workshop allowed discipline-specific experts to identify their main concerns, discuss identified Best Practices, and exchange ideas. The cooperation and sharing that characterised these workshops is the basis for future industry sharing and bodes well for the continued success of such collaborative efforts within the European Union.

Finally, a **three step process was used to arrive at the recommendations** made in this Report. Ideas were generated based on European experiences and collected data from stakeholders. These ideas were then compared against trends and experiences seen in other parts of the world and recommendations were developed. These recommendations were then validated from multiple perspectives to ensure their applicability to a broad range of stakeholders.

In summary, the methodology used throughout the Study is based on proven approaches for similar highly consequential advisory undertakings regarding critical infrastructures. The framework, range of experience and expertise, personal interaction and recommendation process enabled the Study team to delve deeply into the issues facing Europe's future networks, draw upon the knowledge of those most familiar with it, and establish a model for future interaction and sharing.

100 Key Findings of Study

100 Key Findings have been identified relative to the reliability and robustness of future networks. These findings are a combination of European experts' opinions, gathered during face-to-face interviews, virtual interviews, and the four experts workshops, and the expert knowledge and experience of the Study team. The Key Findings form the foundation for the Report's Recommendations.

The Key Findings section also introduces the concept of a five level *maturity model*, that captures the judgements of the experts on the observations produced by the Study. Comments regarding more basic issues invoked little reaction from the experts, indicating that they considered these issues as entry requirements for participation in the industry. Their enthusiasm, however, was tangible when discussing issues that were forward-looking and "ahead of the curve". They believed that addressing these issues was indicative of a world-class communications provider.

The maturity model, described in Section 3, is used to reflect the experts' relative reaction to each Key Finding. For example, those at maturity level 1 are entry-level issues that any provider of communications must address. Those at maturity level 3 are issues that a well established provider of communications services would be expected to address. Key Findings at maturity level 5 include the most challenging issues associated with future networks, and for which solutions may not yet have been developed. The maturity model enhances the presentation of the Key Findings by providing an expert context from which to appreciate the observation.

Three examples of the Key Findings from Section 3 are provided below

Maturity Level 1

4. Future network operators may not be recognised as part of the critical infrastructure

Future network operators may not be recognised as part of the critical infrastructure by Member States or by other industry participants. Conversely, new entrant network operators may not realise that they are part of the critical infrastructure.

Impact: If government and other critical stakeholders do not recognise new entrants as part of the critical infrastructure, the new entrants will not be granted priority treatment in times of crisis. This weakens the robustness of the new entrants' networks, both for their subscribers and for services they may provide for other network providers. Also, without new entrants realising their own critical role, they may not appropriately plan, invest and maintain vital emergency preparedness and disaster recovery capabilities.

Maturity Level 3

28. Priority calling for critical communications in public networks is needed

Many Member States do not have priority calling schemes that allow critical communications over public networks. Even where separate emergency networks exist, there is often a need to provide called or calling party access to public networks. Public networks are also a backup when the separate emergency network sustains damage or is in overload.

Impact: To the extent that critical calls are attempted on public networks, the probability of call completion is not consistent with the urgency of such calls if they are not provided preferential treatment on public networks. The use of public networks provides the critical stakeholders with ubiquitous access, extra capacity, and resiliency.

Maturity Level 4

60. Emergency exercises are essential in preparing for disasters, but are not being sufficiently utilised

Periodic testing of emergency plans is not a common practice for most network operators. Most service providers believe they have some type of plan, but for some companies, this only exists as a general mental picture and is not routinely practiced.

Impact: Emergency response plans must be flexible enough to adjust to specific situations, however the only way to verify the framework of a plan is to periodically exercise it. Exercises also provide the people who participate in them with valuable experience that enables them to provide a much quicker and more efficient response to emergency incidents.

10 Recommendations of Study

Summarised below are the ARECI Study's ten Recommendations for improving the availability and robustness of future European networks. In this executive summary, each Recommendation is presented with an *abbreviated* context, consisting of a brief introduction to the issue, a purpose statement and summary of the commitments required by the Private Sector, Member States and European Institutions. Each Recommendation is supported with a mixture of the Key Findings, knowledge and experience of the Study team, and validation by European stakeholders. Each Recommendation is presented in Section 4 with a more complete context (Figure 1).

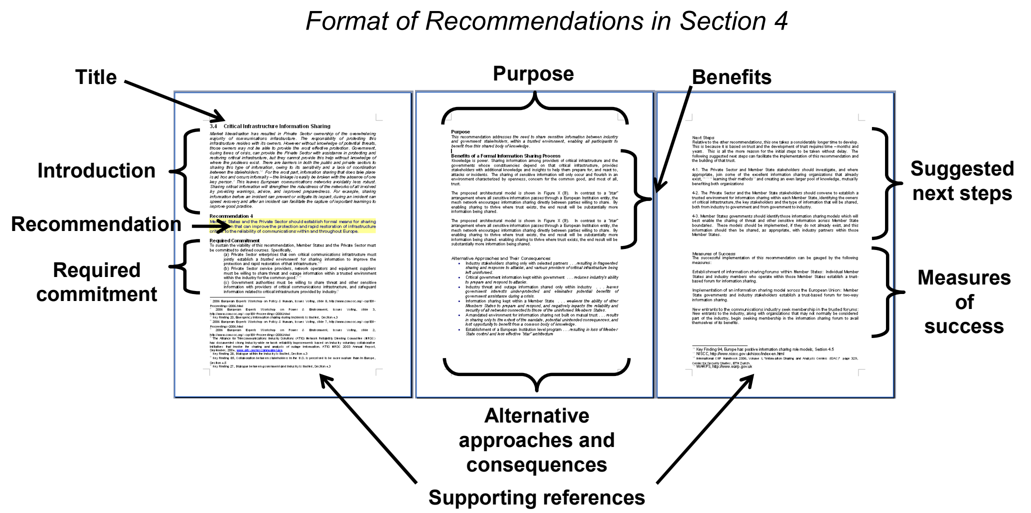


Figure 1: Presentation of Recommendations in Section 4

1. Emergency Preparedness *improve the speed of response*

Issue

The effort expended in preparing for disasters is too often insufficient. Specifically, it is disproportionate in relation to the critical services (public safety, economic, nation-state security) that depend on it. Current programs too often lack involvement of respective Member State governments and coordination at a regional or European level, and are bereft a formal prioritised restoration scheme.

Purpose

This Recommendation is aimed at *improving the speed of response to crisis situations by making as many decisions as possible before the crisis occurs*. If implemented, its impact will be to strengthen infrastructure robustness by better preparing for unknown stress conditions and improving network availability by reducing the time required to restore services.

Recommendation

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.

Required Commitment

The effective implementation of this Recommendation requires the commitments of both the Private Sector and Member State governments. Private Sector companies must be willing to conduct periodic emergency exercises within their own organisations and then with industry peers, and with other sectors. Member State governments and European Institutions must be willing to support Private Sector exercises and commit the resources necessary to efficiently interface with network operators and service providers during a crisis. In addition, the Private Sector and Member State governments should jointly convene analysis groups following emergency incidents to study the response to those incidents, identify key learnings, and to modify emergency response plans based on those learnings. The Private Sector and Member State governments must identify critical services and develop formal plans, including removal of legal barriers if necessary, for providing priority restoration to those services during crisis situations. In addition, the support of European Institutions is needed.

2. Priority Communications on Public Networks *vital calls are not blocked*

Issue

Disaster or other emergency situations usually result in a significantly elevated level of network traffic. While legacy networks could experience service blockage due to traffic congestion, the management of limited network bandwidth will be even more challenging in future networks due to their unpredictable nature. During these crises situations, certain communications are simply essential for saving lives and property, and maintaining social and economic stability, as recovery occurs. First responders and other government authorised users entering the disaster area need to be able to effectively communicate with each other, with other agency responders in the theatre of operation and between the disaster area and the “outside.” The more diverse communication tools that can be rapidly deployed during a disaster situation, the greater the probability to successfully address the communication challenges. Public networks are more ubiquitous than a separate network and a priority scheme can be integrated into the architecture of future networks so that the public networks can be used to extend emergency communications capabilities.

Purpose

This Recommendation addresses the issue of *how to maximise the probability that the most essential communications are completed during periods of high traffic*. This capability focuses on the aspect of robustness that retains the most critical functions during periods of stress.

Recommendation

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.

Required Commitment

In order for this Recommendation to be implemented, the Private Sector, European Institutions and Member State regulatory bodies must work together as equal partners to ensure the proper focus on this critical need. Because the primary stakeholder for priority communications capabilities is the government, normal market forces are not at play and do not produce sufficient motivation for the Private Sector to invest in their development, deployment and maintenance. Therefore, the most crucial commitment is that the Member States are allocating funds to support such investment by the Private Sector. In addition, the Private Sector and Member States need to participate in standards bodies to ensure that the requirements developed by these bodies meet all the unique needs of the European Union Member States. European Institutions may be needed to support facilitation resolution of those issues arising from interoperability of a priority communications capability that spans Europe and supports interoperability with the international community. This may take the form of the articulation of a vision for the key attributes of such a capability and the resolution of conflicting priority schemes among Member States. Finally, the development of such capabilities requires long-term commitment from the Private Sector and should not be directed as unfunded government mandates. With this funding, the Private Sector should develop, deploy, and implement the priority services. To ensure a well-coordinated European capability, both the government funding and Private Sector implementation of functionality should be done incrementally, as the various standards bodies define it.

3. Formal Mutual Aid Agreements *enhance network resilience*

Issue

Mutual aid between companies can greatly extend the robustness of their networks for a relatively low cost. However, while there are some few exceptions, mutual aid in Europe is not widely practiced. Further, when mutual aid is practiced, it is largely ad hoc and susceptible to failure – especially during times of stress

Purpose

This Recommendation addresses the issue of *how to significantly extend the robustness and resiliency of any given network through the shared resources of other industry stakeholders.*

Recommendation

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.

Required Commitment

The effective implementation of this Recommendation requires commitment from the Private Sector and governments. First, Private Sector service providers, network operators and equipment suppliers must acknowledge and accept their reasonable responsibility for maintaining critical services that directly impact social well-being and nation-state security. Secondly, the Private Sector must be willing to offer resources to help competitors in times of crisis. Thirdly, they must consider executing mutual aid agreements with a wide range of industry participants, including non-traditional entities that comprise the European critical infrastructure. On the public sector side, government entities – especially local – must provide communications workers with priority access to disaster sites and assistance in procuring and moving necessary materials (e.g., fuel). Finally, the European Institution and Member State governments must encourage industry cooperative efforts by removing legal barriers to mutual aid for crisis situations.

4. Critical Infrastructure Information Sharing *informing each other*

Issue

The concept of sharing critical infrastructure information is not new to the communications industry in Europe. In fact, the Study team's judgement is that some of the best processes reside in parts of Europe. However, on the whole, the practice is largely underutilised as an instrument for infrastructure protection. This leaves European communications networks avoidably less robust. For the most part, information sharing that does take place is ad hoc and occurs informally – the linkage can be easily broken with the absence of one key person.

Initiatives promoting information sharing must proceed carefully. Member State governments, while committed to the European Union, are also firm regarding their primarily role in the sovereign defence of their nation-state and thus their critical infrastructure. In addition, the European community is a large one. Since trust is ultimately based on individuals trusting other individuals, there are practical limitations on how many trusted relationships can be maintained by any given person.

Sharing critical information will strengthen the robustness of the networks of all participants by providing warnings, advice, and improved preparedness. For example, sharing information before an incident can prevent or mitigate its impact, during an incident can speed up recovery and after an incident can facilitate the capture of important learnings to improve good practice.

Purpose

This Recommendation addresses *the need to share sensitive information between industry and government stakeholders, within a trusted environment, enabling all participants to benefit from this shared body of knowledge.*

Recommendation

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.

Required Commitment

The effective implementation of this Recommendation requires the commitments of both the Private Sector and Member State governments. Entities that own critical communications infrastructure must jointly establish a *trusted environment* for sharing information to improve the protection and rapid restoration of that infrastructure. This may include sharing threat and outage information within the industry. Government authorities must be willing to share sensitive information with providers of critical communications infrastructure, and safeguard information related to critical infrastructure provided by industry. Member State governments must be willing to share information that will improve the protection and rapid restoration of critical infrastructure with other Member States as well as the providers of that infrastructure within those other Member States.

5. Inter-Infrastructure Dependency *critical sectors working together*

Issue

Critical infrastructures, which play a major role in the economic, physical and cyber well-being of Europe, form a complex “system of systems.” Critical infrastructure protection is at varying stages of being addressed in the Member States and the European Institutions. Interdependencies are complex and need to be understood since disruptions in one infrastructure can propagate into other infrastructures. While specific critical infrastructure protection and recovery responsibilities are primarily local, they may have a European-wide impact.

Purpose

This Recommendation is aimed at *enhancing the availability and robustness of Europe’s critical infrastructures by identifying and addressing sector interdependencies*.

Recommendation

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.

Required Commitment

The required commitment to implement this Recommendation is high in terms of both expert skills, resources and long term vision. Communications service providers and network operators need to recognise their interdependencies with other critical sectors, and appropriately support efforts to better understand and manage those interdependencies. The Private Sector, European Institutions and Member States must continue to work together to understand and develop their specific roles to ensure the proper focus and level of effort and coordination for these initiatives. European Institutions and Member State governments must be willing to fund research to address aspects of interdependencies insufficiently understood. The research community must provide solutions to substantially strengthen the understanding of critical sector interdependencies and enable effective management of complex and dynamic interactions.

6. Supply Chain Integrity and Trusted Operation *clean networks*

Issue

It is well understood that competitive pricing pressures have motivated software and hardware businesses to seek the most cost-effective methods of producing their products. A trade-off of this trend was apparent in this Study: One of the most consistent messages voiced throughout the Study's stakeholder engagements was concern for the integrity of software supply chains. Three factors come together to drive this concern. First is the *speed at which the shift to outsourcing* has taken place. The concern is that appropriate quality and other controls have not been put in place to protect against challenges beyond quality defects – namely malicious influence in the outsourcing process. A second factor is the *increased risk brought through dependency on software-controlled technology*. Society, businesses and critical nation-state interests have grown dramatically more reliant on such technology for basic function and survival – even when compared with just a decade ago. The third factor is the *global security environment* with numerous security aspects viewed as having a harmful influence on the integrity of supply chains. These aspects include the mode of asymmetrical terror attacks against the interests of stable societies is consistent with cyber terrorism, the electronic interconnectedness of the world enables "triggers" to be pulled from anywhere in the world, and the relative instability of some geographic regions could jeopardise the ability to attain timely technical support for products developed in those areas, should there be a regional problem. Stakeholders expressed similar concerns for hardware, though to a lesser degree. In addition, the networks in which these hardware and software products are deployed will require the development of innovative trust conceptions to ensure the integrity of network operations.

Purpose

This Recommendation is aimed at *providing hardware and software supply chain technology and assurances of integrity* regardless of where or by whom, the technology was designed, developed, manufactured, or deployed. It is further aimed at *operating future networks with safeguards that provide assurances of trustworthiness*, regardless of their owner or operator.

Recommendation

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.

Required Commitment

The required commitment to implement this Recommendation is high because of differences between the everyday visibility of concrete competitive pricing pressure, which the consumer enjoys, and the less tangible reality of the factors described above. European Institutions and Member States must face their vital dependence on Information and Communications Technology (ICT) and articulate a vision that properly stresses the importance of trusted hardware, software and networks. In addition, European Institutions and Member States should encourage, by policy and economic incentive, research that supports the development and implementation of supply-chain processes and safeguards that provide assurances for technology trustworthiness. Further, European Institutions and Member States should provide incentives for Private Sector investment by awarding government communications services contracts to those service providers most aligned with these principles to improve security and reduce vulnerabilities. Finally, the Private Sector needs to continuously pursue technology improvements in the quality and control of their supply chains across the product lifecycle (e.g., design, development, deployment, support) to increase the security assurance of information and communications systems.

7. Unified European Voice in Standards *more clout for unique European needs*

Issue

The benefits of industry standards are interoperability and reduced costs. However, the use of standards also introduces hazards such as reliance on outdated standards, conflicting standards from different bodies, misinterpreted standards and overlapping standards from different bodies. These issues have a negative impact on network availability in three ways. First, not all services are available on all networks because of different standards being followed. Secondly, networks can fail to interoperate as anticipated. Thirdly, incompatibilities can appear when networks are under unexpected stress. The challenge of “getting standards right” will be even greater in future networks as the number of players increases and the pace of network technology development and deployment accelerates. Fortunately for Europe, the growing collaboration among Member States brings with it opportunities for better coordination in its standardisation pursuits.

Purpose

This Recommendation is aimed at *promoting network availability by reducing conflicts* between network operators, service providers, equipment suppliers, and between networks operating across Member States’ boundaries by adopting common standards. Coordination at standards bodies strengthens the European Union influence and ensures that the standards meet the unique needs of the European community.

Recommendation

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.

Required Commitment

Member States and Private Sector service providers, network operators and equipment suppliers must embrace the need to establish standards that will benefit the European communications industry as a whole. Member States, with the active support of private industry, must represent its constituents with one voice to increase the joint influence of the European communications community.

8. Interoperability Testing *a level playing field*

Issue

Future networks will involve many more network operators and service providers connecting to each other. However, the procedures for determining the viability of new networks before interconnecting to existing networks are inconsistently defined by each interconnecting network provider. This is a potential source of conflict between network operators that could cause network failures or other impairments affecting service availability. Currently, network interface testing varies greatly among network operators.

Purpose

The *reliability of future networks can be enhanced by having an agreed upon set of tests that would be executed prior to the connection* of a new network to existing networks. Since a network is only as viable as the weakest element, this testing framework will help to ensure the integrity of future networks. A standardised testing framework would ensure an expedited validation process, and reduce disputes regarding test results. This testing framework provides a systematic and comprehensive method of validating all the various necessary operations.

Recommendation

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.

Required Commitment

The effective implementation of this Recommendation requires the commitments of both the Private Sector and Member State governments. The Private Sector must embrace the need for a standardised network-to-network testing framework. In addition, Member States must recognise a standardised testing framework as a reasonable means for determining the readiness of networks to be interconnected**.**

9. Vigorous Ownership of Partnering Health *it is my responsibility*

Issue

Optimum availability and robustness of European networks can only be achieved through effective partnerships between the Private Sector, Member States and European Institutions. However, one of the most frequently raised issues, and most strongly expressed, by stakeholders during the Study was dissatisfaction with current collaborative efforts between the Private Sector and government. Some role models of communications sector collaboration exist, but they are rare. The symptoms presented throughout this Study's vast engagement with stakeholders lead to the diagnosis that too often, critical public private partnerships are suffering from suboptimal health. Both private and public sector stakeholders are concerned that the type of equal partnership needed to face the emerging challenges of future networks has not been attained.

Purpose

This Recommendation addresses the issue of how each party of a critical public-private partnership can break through the impedance that too often stifles necessary collaboration, and thus wastes opportunities to *collectively advance common interests regarding network availability and robustness.*

Recommendation

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.

Required Commitment

The effective implementation of this Recommendation requires the commitments of the Private Sector and European Institution and Member State governments. The Private Sector must recognise that government regulators and other government stakeholders have responsibilities for industry oversight and protection of specific public interests, and that its support is necessary in order for these responsibilities to be effectively and practically carried out. Further, the Private Sector must recognise the government's need for selected information relative to its oversight role and other responsibilities, without compromising security or competitive business interests. Government regulators and government stakeholders must respect Private Sector business interests and their need for protection of any information voluntarily shared, such that policies and practices are established and strictly followed to facilitate an environment of trust. In addition, the Private Sector, Member States and European Institutions should set realistic expectations for the nature of public-private partnerships, given that ongoing tensions and rigorous debate on matters of interest and policy are expected and healthy. Finally, the Private Sector, Member States and European Institutions should each accept responsibility for the current and continued health of the partnership.

10. Discretionary European Expert Best Practices *harnessing expertise*

Issue

Achieving highly available, highly robust and highly secure communications networks depends heavily on technical and operational expertise. Communications infrastructure ownership, and thus this expertise, lies primarily in the Private Sector. It is critical to engage and harness this expertise as best possible. Industry consensus best practices, distinct from standards and regulations, are an underutilised method in Europe, yet they are the most effective way to capture expertise and make it available to the broader industry. One of the milestones achieved during this Study was the confirmation by European experts of a core set of voluntary Best Practices that promote network reliability and security.

Purpose

This Recommendation addresses the issue of *how to ensure that the best expertise is engaged in promoting the availability and robustness* of Europe's electronic communications infrastructures. Appreciation for the value of voluntarily-implemented, industry-consensus Best Practices comes from understanding both the nature and vital role of expertise in this sector.

Recommendation

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.

Required Commitment

The effective implementation of this Recommendation requires the commitments of the Private Sector and Member State governments and European Institutions. The Private Sector must initiate collaboration to share expertise, develop consensus on Best Practice guidance, maintain the collection of this guidance, and take seriously their responsibility regarding the voluntary implementation of Best Practices. Government powers must respect the Private Sector Best Practice development process as not intended to be one in which ideas and principles shared can be used against those contributing them. Government powers must therefore abstain from using Best Practices collaboration efforts as a step toward regulation. The Private Sector, Member States and European Institutions must work together as equal, trusted partners to ensure the proper focus and level of effort for these initiatives.

Summary

This Study submits ten major Recommendations to European Institutions, Member States and the Private Sector for the express purpose of promoting the availability and robustness of Europe’s communications networks. These ten Recommendations are submitted specifically to the European Commission for their consideration and inclusion in their ongoing dialogue regarding how to achieve the communications infrastructure availability and robustness needed by Europe. The Study team strongly urges the European Commission to include this report in its dialogue and to do so speedily, as the improvement opportunities described have many benefits to European citizens. Further, the Study team strongly urges the Member States and Private Sector to likewise include consideration of this report in their respective undertakings addressing network availability and robustness. The Study team is encouraged that at the time of this report’s final drafting, a number of Private Sector stakeholders have stepped forward to take the next steps suggested for several Recommendations.

Each of the Recommendations should be considered and acted upon with urgency proportional to the vital role that communications networks will play in Europe’s future. The *critical* priority for implementation is clear. Without reliable communications networks and services, public welfare is endangered, economic stability is at risk, other critical sectors are exposed, and nation-state security is threatened. The implementation of this report’s Recommendations will significantly reduce these and other risks. Each of the ten Recommendations is both challenging and achievable. The Study team’s interest extends beyond documenting the guidance found herein. The intent is that the result of improved network availability and robustness would be realised. Successful implementation of each Recommendation will significantly improve the reliability and robustness of communications services for the citizens of Europe. However, each will require skill, resolve and genuine partnership among government entities and the Private Sector. To help the process of taking these Recommendations from paper to results, each is supported with a complete background, with a discussion of less desirable alternatives, with next steps to continue established momentum from the Study, and with measures of success where stakeholders can benchmark their effectiveness in supporting the guidance (Section 4). These value-adding elements are included to these Recommendations because of the *criticality* and *urgency* regarding their implementation.

Europe’s future communications networks promise to usher in a new world of business and lifestyle-enhancing capabilities – many of which have not yet even been imagined. Relatively recent advances of ICT in the areas of affordable pricing, mobility, geo-locating, video imaging and search engines, while breathtaking, are likely only the beginning of an ever-accelerating pace of the same for the foreseeable future. While the urgency is pressing, the long term benefits of reliable communications networks are incomparable. The people of Europe stand to greatly benefit from the anticipated economic efficiency, citizen connectivity, functional flexibility, and speed. This Study strongly urges the European Commission, Member States and Private Sector stakeholders to chart and embark on a new course of policy and practice that forcefully advocates highly available and highly robust communications infrastructure.

This page is intentionally left blank

2 INTRODUCTION

This section provides explanatory information for the Study. It includes the Study's mission, scope, terms of reference and methodology. The Study team collected and analyzed in excess of 30,000 data points. This section details the sources and types of data collected and the approach used to learn from it. This description lays the foundation for the heart of the Report: Key Findings (Section 3) and Recommendations (Section 4). Additional background on technology, future network architectures, and threat modelling analysis can be found in the annexes.

2.1 Mission

European security, economic stability and prosperity, and the public safety and welfare of its citizens, increasingly depend on the availability and robustness of its electronic communications infrastructures. The operation of critical sectors such as finance, energy, transportation and government are more and more dependent on communications networks with each passing month. The rise in average living standard is highly correlated to the availability and associated efficiencies of communications networks. The trade-off for these many benefits is *living with the continual dependence on these networks*. Thus, they need to be highly available. This dependence is acceptable to the degree that high network availability and robustness are achieved. This Study is focused on this crucial subject of end-to-end network availability and robustness. European citizens are used to the high reliability of legacy telephone service and come to expect new services (e.g., VoIP, Internet, IPTV) to have a similar level of reliability.

The following statement represents the purpose of this Study:

> **The aim of the present Study is to develop a forward-looking analysis of the factors influencing the availability of electronic communication networks and of the adverse factors acting as potential barriers to the development of global networked economies by lowering their dependability.**[1]

2.2 Scope

The scope of the Study was determined very carefully. The title of this Study defines its scope as dealing with the *availability* and *robustness* of *electronic communications infrastructures*. This section provides some straightforward and plain statements that clarify what is meant by these terms. Further, the scope is carefully articulated here based on the documented European Commission guidance for this Study and the global communications industry's use of referenced terminology.

2.2.1 Terms of Reference

The expectations for communications services are very high. Numerous terms are routinely used by the communications industry to refer to these high expectations and to distinguish between particular attributes of the expectations and needs of users. Following is a brief discussion of the terms *availability* and *robustness*.

[1] Tender Specifications, A Study on Availability and Robustness of Electronic Communications Infrastructures, Modinis Workpackage: Wp4.2, 2005, *Objective of the Study.*

Availability is simply the extent to which a system is ready to be called into use for its designated purpose, without advance knowledge of when it is needed.[2] In this Study, the system is Europe's electronic communications infrastructures, which are made up of many networks.

Robustness is the property of being strong and healthy in constitution.[3] It is further defined as a condition of a system design "that remains relatively stable, with a minimum of variation, even though factors that influence operations or usage, such as environment and wear, are constantly changing."[4] Robustness is the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environment conditions.[5]

The meaning of this term is worth further consideration. Other definitions vary in (a) the emphasis they place on *where the challenges come from* - internal (e.g., component failure) or external (e.g., environmental), (b) *the degree to which such challenges are anticipated* - ranging from conditions slightly beyond what is expected to anything unexpected, and (c) the *level of stability of functionality maintained* during the period of stress. For the purpose of this Study, the robustness of electronic communications infrastructures includes:

- the ability to maintain *critical* functions, but not all functions
- in the context of *both internal and external* challenges
- when the challenges are of any *degree of variability from expected conditions*, but that expectations should diminish with increased stress (e.g., a more robust system can handle more extreme forms of stress)

Related terms include *reliability*, *dependability*, *resilience* and *survivability*. Network *security* relates to the subject matter in that compromises of security can cause infrastructure failures.

Communications infrastructure is defined as "organisations, personnel, procedures, facilities and networks employed to transmit and receive information by electrical or electronic means."[6] The notion of "electronic" is inherent to this definition.

A complete list of the ingredients of communications infrastructure includes eight items:[7]

- **Environment:** Communications systems are in the physical universe and as such, operate in various environments. These environments range from temperature-controlled buildings to installations exposed to harsh conditions such as outside terminals and cell towers that are exposed to inclement weather, trenches where cables are buried, space where satellites orbit, and the ocean where submarine cables reside.

- **Power:** Without electrical power, electronic systems are lifeless. The power required for communications networks includes the internal power infrastructure, batteries,

[2] A more formal definition: The degree to which a system, subsystem, or equipment is operable and in a committable state at the start of a mission, when the mission is called for at an unknown (i.e. a random) time.
Glossary contains a more complete definition, including mathematical formula.

[3] wordnet.princeton.edu/perl/webwn.

[4] www.onesixsigma.com/tools_resources/glossary/glossary_r.php

[5] Institute of Electrical and Electronics Engineers. *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.* New York, NY: 1990.

[6] www.bitpipe.com/tlist/Telecommunications-Infrastructure.html.

[7] K. R. Rauscher, R. E. Krock, J. P. Runyon, "Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security" Bell Labs Technical Journal, 11(3), 73-78 (2006) ©Lucent Technologies Inc. Published by Wiley Periodicals Inc. Published online at Wiley Interscience (www.interscience.wiley.com).

grounding, cabling, fuses, back-up emergency generators and fuel, and commercial power.

- **Hardware:** The electronic and physical components that comprise the network nodes, including the hardware frames, electronics circuit packs and cards, metallic and fibre optic transmission cables, and semiconductor chips.

- **Software:** Today's complex communications networks gain their power and flexibility from the computer code that controls the equipment. This category covers all aspects of creating, maintaining, and protecting that code, including physical storage, development and testing of code, version control, and control of code delivery.

- **Networks:** Networks include the various topological configurations of nodes, synchronisation, redundancy, and physical and logical diversity.

- **Payload:** The purpose of a communications network is to deliver some form of communications, be it voice, data, or multimedia. The payload category includes the information transported across the infrastructure, traffic patterns and statistics, information interception, and information corruption.

- **Human:** Humans operate the network and present one of the most complex dimensions to analyze. The human ingredient includes intentional and unintentional behaviours, physical and mental limitations, education and training, human-machine interfaces, and personal ethics.

- **Policy (or ASPR):** Policies include any agreed or anticipated behaviour between entities, such as companies or governments. They include agreements, standards, policies and regulations (ASPR) and provide a framework that defines the expected interaction between government and the communications industry.

The authors of this Study employed a framework built on these eight ingredients of communications infrastructure to structure their study (Figure 2). This framework has been very helpful in numerous industry-government-academic collaborative efforts.[8] The framework was used to develop a comprehensive list of intrinsic vulnerabilities of existing and future networks, identify factors that could influence national-level network reliability, assess the critical components of an emergency ad hoc network, and develop industry-consensus network reliability, network security and homeland security best practices that are widely-deployed.[9] This framework is comprehensive in the sense that all the ingredients needed for the full operation of a communications network are included. The framework also recognises the role of other sectors.

[8] Rauscher, Karl F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004; Rauscher, Karl F., Krock, Richard E., Runyon, James P., *Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security* Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004.

[9] The President's National Security Telecommunications Advisory Committee Next Generation Networks Task Force Report, March 28, 2006, *Background and Charge, Appendix G;* ATIS Network Reliability Steering Committee (NRSC) *2002 Annual Report* (www.atis.org/nrsc); Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop, Rancho Bernardo, CA, USA, (www.comsoc.org/~cqr); Proceedings of the 2006 IEEE Communications Society CQR International Workshop, London, U.K. *Wireless Emergency Response Team*; Federal Communications Commission (FCC) Network Reliability and Interoperability Council (NRIC) VI *Homeland Security Physical Security Focus Group Final Report*, Issue 3, December 2003; NRIC VII *Wireless Network Reliability Focus Group Final Report*, Issue 3, October 2005; NRIC VII *Public Data Network Reliability Focus Group Final Report*, Issue 3, October 2005 (www.nric.org).

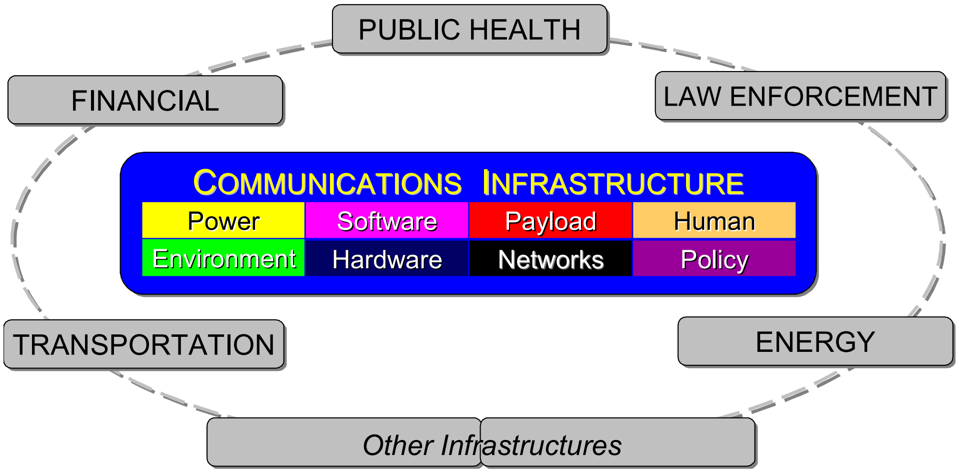


Figure 2: Eight Ingredient Framework of Communications Infrastructure

2.2.2 Network and Technology

This Study covers a wide range of networks, technologies, standards and services. The following descriptions will be helpful to readers trying to determine whether the Study's guidance is applicable to specific types or networks, technologies or services.

Network Access Types

This Study considered the following network access types:

- cable (coaxial cable)
- optical (fibre optic cable)
- wireless (air interface)
- wireline (copper wire)

Annex E provides a technical description that includes these network types. Each of these networks, circuit-switched, packet-switched and converged technologies are included. More specific details are listed in the next section.

Network Technologies

This Study considered the following alphabetically-listed technologies, which include communication platforms, protocols and standards. Some of these technologies are inclusive of others. The list is provided to show the diversity of networks used in Europe and thus considered in the Study:

- Asynchronous Transfer Mode (ATM)
- Broadband Wireless Access (BWA)
- Data Over Cable Service Interface Specification (DOCSIS)
- Code Division Multiple Access (CDMA)
- Global System for Mobile communication (GSM)
- Intelligent Network (IN)
- Internet Protocol (IP)
- IP Multimedia Subsystem (IMS)
- Next Generation Networks (NGN)
- Session Initiation Protocol (SIP)
- Signalling System 7 (C7, SS7)
- Synchronized Optical Networking (SONET)

- Synchronized Digital Hierarchy (SDH)
- Third Generation Wireless (3G)
- Time-Division Multiplexing (TDM)
- Wireless Fidelity (WIFI) IEEE 802.11
- Wireless Local Area Network (WLAN)
- Worldwide Interoperability for Microwave Access (WIMAX) IEEE 802.16
- Universal Mobile Telecommunications Service (UMTS)

Annex E provides a technical description that includes many of these network technologies.

Subscriber Service Types

This Study also considered the complete spectrum of subscriber services. A review of this list of services supports several important observations. First, it includes both old and new services. Throughout the Study, consideration had to be given to promoting availability and robustness for three situations: legacy networks, future networks[10] and the converged networks, which require both legacy and future networks to operate together. Second, the nature of the services includes attributes that are very different and thus require appropriate consideration. For example, traditional voice service has a relatively predictable and small use of bandwidth and requires real-time transmission. In contrast, most data services have a highly *un*predictable bandwidth need and have no real-time transmission support. Still, some video, gaming or conferencing applications may require both high bandwidth and real-time transmission support. The Study team factored in the attributes of each of these service types:

- Data
- Voice
- Text
- Video
- Simultaneous Multi-media
- Instant Messaging
- Internet
- Priority (emergency)
- Conferencing
- Gaming

Annex E provides a technical description and context for the provision of these service types.

2.3 Principles of Approach

Seven principles guided the manner in which this Study was conducted and were thus instrumental in formulating the final Recommendations:

- *Keep the interests of the citizens* of Europe in the forefront
- *Be forward-looking* in technology considerations, factoring in trends
- Uphold *European focus*, yet maintain global awareness
- *Be inclusive* in receiving all European insights offered

[10] The term “future networks” is used to refer to the many types of emerging network architectures and technologies. The popular term “Next Generation Networks” or “NGN” is avoided in this report so as to not assume the context of an incumbent (i.e. one who already has an existing network).

- *Ensure rich representation* of industry, academic and government perspectives, with care to include both embedded as well as new entrants
- *Utilise world-class proficiency* in both the technical subject matter and broader policy areas to ensure the output would be both realistic and achievable
- *Fulfil the formal requirements* for the Study's execution

Because the interests of the European citizen were at the forefront, there is an emphasis on lifeline and emergency public safety communications, as addressed by Recommendation 2, *Priority Communications on Public Networks*. The Study's forward-looking posture is reflected in that over half of the Key Findings deal with specific issues of future networks. The European focus was maintained by limiting the definition of stakeholder to one operating within at least one of the EU Member States. To provide the desired insights from other global regions, the core team consisted of experts with vast international experience. To be inclusive of all European insights, the Study team held open experts workshops and conducted interviews in numerous cities across Europe. The team also employed electronic virtual interviews to further reach out for many perspectives. Care was taken to seek balanced representation. The next section outlines the vast representation of perspectives. Finally, the Study was conducted by senior experts with relevant competencies. The team's leadership has a demonstrated track record of critical government-industry collaboration leading to successfully implemented recommendations that have been measurably demonstrated to greatly improve network reliability.[11]

2.4 Participants

Two of the guiding principles of this Study focused on *being inclusive regarding perspectives* and *seeking representative perspectives*. This section provides more details on how these very important principles were fulfilled.

One of the *most distinguishing aspects* of this Study was the *rigorous engagement with industry expertise.* This rigorous interaction culminated in four experts workshops convened to allow experts to interact with their peers concerning each of the eight ingredient areas (Figure 2). This Study received the support of over 80 organisations and had direct contact with over 200 of Europe's best subject matter experts from all levels of organisational hierarchy – ranging from engineers, to middle managers, to corporate officers. In addition to individuals directly engaged in supporting the Study, additional experts were consulted within these organisations. The organisations spanned the Private Sector, academia, government and each Member State (Table 1). Individuals supporting this Study contributed in numerous ways:

- deliberated deep technical and policy issues
- identified *intrinsic vulnerabilities of utmost concern* for future networks
- evaluated specific *Best Practices for effectiveness* in European networks
- evaluated specific *Best Practices for risk to not implement* in European networks
- evaluated specific *Best Practices for cost to implement* in European networks
- identified the *implementation status of specific Best Practices*
- participated in rigorous interactive workshops with other industry experts
- came to *consensus with peers on the highest priorities* for network availability
- came to *consensus with peers on best approach* for addressing concerns

[11] Biographies of the Study team are provided in Section 7.

Table 1 lists the subset of organisations that contributed to this Study or participated in the public forum. In addition to the 124 organisations listed, numerous other organisations contributed whose names are not listed.

Table 1: Organisations that contributed to the Study

AGH (Akademia Górniczo - Hutnicza) University of Science and Technology
Alcatel-Lucent
ALCATEL-LUCENT BELL LABS
AMS-IX
Ancitel Sardegna
Austrian Association of electricity companies
Belgacom
Belgian Institute for postal services and telecommunications
BELTUG
Blekinge Institute of Technology
British Library
BT
BT Italia
BT Wholesale
Bulgarian State Agency for Information
Bundesministerium des Innern (German Federal Ministry for the Interior)
Centr
CIVIL CONTINGENCIES SECRETARIAT – UK CABINET OFFICE
Clusit
Commission de Surveillance du Secteur Financier (CSSF), Luxembourg
Cyber Security Industry Alliance
CYTA
Hungarian Department for International Relations
Deutsche Bahn
Deutsche Telekom AG
DG ENTR
DG INFSO
DG JRC
DG TAXUD
DG TREN
DHL Europe
DISSC, Spanish Prime Minister's Office
Dutch Ministry of Economic Affairs
EastWest Institute
Elsinore
ENEA
ENISA
ENISA MB Alternate UK member
Ericsson AB
ETNO
ETSI
Eurescom GmbH
Euro Cablelabs
EuroISPA
European Telecommunications Standards Institute (ETSI)
Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway, Germany

Federal Office for Information Security (BSI), Germany
Federal Reserve System, USA
France Telecom Group
French Ministry of finances and industry
Ghent University
Govt. of Luxembourg (Nat. Sec.)
Hellenic Telecommunications Organization (OTE)
Helsinki University of Technology (HUT)
High Institute for Communications and Information Technologies, Italy
Hungarian Prime Minister's Office
Iberdrola
ICP-Anacom
IIAT
Infineon Technologies
Initiative Europäischer Netzbetreiber
Interxion
INTUG
Juniper Networks
KPN
LanditD Ltd
LogicaCMG
Magyar Telekom
McAfee
Microsoft
Ministry of economy, Slovenia
Ministry of Government administration and reform, department of IT policy, Norway
Ministry of Industry, Tourism and commerce, Spain
Ministry of informatics of the Czech Republic
Ministry of interior Lithuania
Ministry of Transport and Communications, Norway
Ministry of Transport, posts and telecommunications of the SR
Mission of Japan to the E.U
National Cryptologic Center
National Emergency Supply Agency, Finland
National IT and Telecom Agency, Denmark
NATO
NEC
Net technologies Ltd
Netia S.A.
Netnod Internet Exchange
NISCC / CESG
Nortel Networks
Norwegian National Security Authority
Ofcom
Orange FT
Political Intelligence
Polska telefonia cyfroha sp200
Portugal Telecom
Rohde & Schwarz SIT
SFR
SiConnect Ltd

Siemens networks
SINTEF Energy Research
Spanish permanent representation
SPF Justice
SWIFT
SYMANTEC
TDC
Telecom Italia
Telefonica Deutschland
Telefonica Moviles
Telefonica O2 Cz
Telefonica Spain
TeliaSonera
The Open University
T-Mobile
TP S.A
T-REGS bvba
T-Systems
TVCABO
UKERNA
University of Bristol
US Mission to the EU
Verisign
Verizon Business
Vodafone Italy

Environment & Power Experts Workshop

3 October 2006
Rome, Italy

A.

Network & Payload Experts Workshop

6 October 2006
London, U.K.

B.

Hardware & Software Experts Workshop

11 October 2006
Berlin, Germany

C.

Policy & Human Experts Workshop

15 November 2006
Brussels, Belgium

D.

Figure 3: Consensus Development at Experts Workshops
Hosts: A) Italian Ministry of Telecommunications
B) BT
C) Rohde & Schwarz SIT
D) SWIFT

2.4.1 Private Sector

The Private Sector included both members of the communications industry and those who are critically dependent on it.

Industry Roles
For those directly involved in the communications industry, there are five primary roles: Service Provider, Network Operator, Property Manager, Industry Association, and Equipment and Solutions Supplier. The following is a brief definition of these roles.[12] It is important to be inclusive of each perspective as infrastructure availability and robustness is dependent on many players. To not include the insights of all those involved would leave important information and interest inappropriately out of the analysis process.

> ***Service Providers*** are organisations that provide communications-based offerings directly to subscribers. The primary business model is typically that of providing network access (or connectivity) for subscribers, content hosting or distribution, or the handling of private messages (e.g., news server). The Service Provider may or may not be the operator of the network.[13]
>
> ***Network Operators*** are organisations responsible for the development, provision and maintenance of real-time networking services and for operating the corresponding networks. Most of the organisations are for-profit businesses, however some operate as not-for-profits.
>
> ***Property Managers*** are the entities responsible for the day-to-day operation of any facility (including rooftops and towers), and are usually involved at the macro level of facility operations and providing service to a communications enterprise. This responsibility may include lease management, building infrastructure operation and maintenance, landlord-tenant relations, facility standards compliance, and common area maintenance and operation, which may include base building security and reception.[14] Network Operators often serve in the Property Manger role when their buildings are needed as locations to make network connections.
>
> ***Industry Associations*** are those entities that provide as their primary function the organisation of industry interests across multiple organisations. Most such organisations are not-for-profits.
>
> ***Equipment and Solutions Suppliers*** are organisations whose business is to supply network operators and service providers with equipment, software or services required to deliver reliable network service. Suppliers of consumer end-user devices are increasingly included, as those devices are an integral part of future networks.

Sector Stakeholders
Every critical sector is dependent upon communications networks. The nomenclature, and thus number, of sectors varies across countries.[15] Most taxonomies recognise the following:[16]

[12] Network Reliability and Interoperability Council Homeland Security Focus Group Final Report, December 2002, Issue 3, www.nric.org.

[13] A company, organisation, administration, business, etc., that sells, administers, maintains, charges for, etc., the service to consumers.

[14] This role recognises the responsible operational entity, which may be the facility owner or landlord, the majority owner of a shared facility, the owner's representative, a professional property management company, a realty management company, tenant representative (in the case of triple net or like-kind lease arrangement), a facility provider, a facility manager, or other similar positions.

[15] This variation, and a European Programme on Critical Infrastructure Protection (EPCIP), is discussed in Annex D, Communications Networks Interdependencies. Recommendation 5 addresses the need for a consistent European taxonomy.

- Agriculture and Food
- Banking and Finance
- Chemicals and Hazardous Materials
- Emergency (Public Safety) Services
- Energy
- Government
- Health Services
- Information and Communications Technology (ICT)
- Insurance
- Law Enforcement
- Oil and Gas
- Transportation
- Water

2.4.2 Academia

The academic community has an unique perspective that is important to engage for studies such as this. The academic community is often contrasted with industry as being less familiar with the practical aspects of real world network operations. However, university and other research institutions often have an important advantage of *not* being constrained by some of the nearer term business issues that can impede Private Sector research programs. The term, broadly defined, also includes non-education-oriented research institutions.

2.4.3 Government

Government has several important roles concerning network availability and robustness. Before the current trend of privatisation, governments in Europe have played a major role in the operation of communications networks used by the public. Today, several Member States continue to operate separate emergency networks. Other primary roles include that of regulator, stakeholder and researcher.

> ***Government Regulators*** can be a major factor (positive or negative) in influencing the direction, flexibility and pace of technological advances. Regulators have power to control network operators and service providers. They often wrestle with many competing interests. Most regulators have some responsibilities, on behalf of the public, to oversee the availability, quality and reliability of communications services.
>
> ***Government Stakeholders*** range from civil defence and inner security interests, to public safety and other emergency services, to economic interests of the ministries of economic affairs. Many government ministries exist because of their critical role in supporting society, and each of these is increasingly dependent – in a vital way – on reliable and secure communications networks.
>
> ***Government Researchers***, like academia, provide an important, unique perspective on critical sector issues. Government research programs provide an independent view with uniquely public sector interests. These functions are often carried out via academic or Private Sector research partnerships, but with government oversight.

16 International Critical Information Infrastructure Protection (CIIP) Handbook 2004, , An Inventory and Analysis of Protection Policies in Fourteen Countries, Swiss Federal Institute of Technology, p. 345.

2.4.4 Other Aspects of Representation

In addition to ensuring representation from each of the roles described above, other important aspects were also sought. These include:

Technology and Services: Each of the network access types, network technologies and service types was included above (Section 2.2.2).

Business Model: The increased competition across the European communications landscape currently cultivates a diverse set of business models. These include traditional incumbents, new entrants and even non-profit operations.

Disciplines: One of the defining characteristics of this Study is its direct access to subject matter experts. By definition, experts have a very deep command of a specific area. To cover the eight ingredients that make up communications infrastructure (Section 2.2.1), individuals needed to be consulted who were recognised as authorities in their fields in the following essential areas:

- Environment: network maintenance engineers, physical security managers, co-location coordinators
- Power: power system engineers, emergency preparedness and disaster recover managers and executives
- Network: network architects, network operations managers, network evolution executives, network reliability and disaster recovery managers,
- Payload: network security experts, network planners
- Hardware: electrical engineers, physicists, chemists, hardware designers, hardware developers, system engineers, quality managers
- Software: computer programmers, software testers, quality managers, cyber security managers
- Policy: lawyers, corporate government affairs representatives, corporate officers, standards representatives and facilitators, government stakeholder representatives from other sectors
- Human: human performance engineers, personnel trainers

Government Levels: Government representatives were engaged from the entire range of government: European, Member State and local.

Corporate Levels: Corporations were engaged at both the “headquarters” level and subsidiary level. For example, large carriers that were operating separate business within countries other than their home country were included.

Size: The Private Sector organisations and Member States supporting this Study ranged from the very small to very large.

European Union Entrance: Member States were included that represented both EU charter members as well more recent joiners.

2.5 Methodology

The ARECI Study was conducted over a period of approximately one year. The methodology used a custom-designed approach for the special needs of the mission. The special needs of the mission included the following aspects. First and foremost, the work is very important as the availability and robustness of public networks is crucial for many reasons, the most crucial being that it can be a factor in saving lives.

Secondly, because the heart of this Study deals with critical infrastructure, it is of immediate interest for Member States both from a sovereignty and socio-economic perspective. Thirdly, the Private Sector is simultaneously managing increased competition and wide sweeping technological changes. The final aspect is the global security environment that includes both increased concern of terrorist attack and the possibility of a remote cyber attack from another part of the world. The approach designed for this Study addresses these four concerns through various means.

2.5.1 The Eight Ingredient Framework

The eight ingredient framework was used because it brings the advantage of being comprehensive and therefore the most thorough framework for assessing infrastructure concerns. The striking advantage of using this framework is that it readily lends itself to the comprehensive listing of intrinsic vulnerabilities,[17] which are defined as characteristics of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise. Intrinsic vulnerabilities are *finite* – unlike threats, which, for practical purposes, are *infinite*. Present-day security approaches are for the most part founded on the threat side of the equation, which is derived from historic experience and gathered intelligence. In contrast, the intrinsic vulnerability approach, rooted in a detailed knowledge of the ingredients that make up a communications network, permits profoundly higher degrees of confidence in terms of ensuring reliability and robustness. This thoroughness is just what is needed for the foundation to meet the needs related to how important network availability and robustness are to society. The framework is also uniquely effective in defending against terrorist attacks. Because such attacks are based on surprise, the threat side, which is based on gathering intelligence, is always playing catch up. In contrast, the intrinsic vulnerability approach focuses on the other side of the equation, where vulnerabilities are stable and their properties known. The eight ingredient approach was used in the following ways:

- Evaluate emerging networks
- Compare the impact of trends
- Rank stakeholder concerns
- Conduct interactive workshops
- Organise Best Practices
- Contextualise Key Findings

This focus on vulnerability analysis does not exclude the use of threat analysis, which draws extensively on observed trends and the subjective perspectives of individuals. Rather, it uses that knowledge and supplements it with expert knowledge about the systems that make up communications networks.

Intrinsic Vulnerability Analysis

The eight ingredients identified in Section 2.2.1 provide the framework for doing a comprehensive, systematic, and rigorous analysis of future communications networks. As noted in Annex B, identification and mitigation of the vulnerabilities for each of the eight ingredients allows unknown threats to be rendered harmless.

As part of this Study, subject matter experts were polled as to which of the intrinsic vulnerabilities (complete list provided in Annex B) caused them the greatest concern

[17] Annex B.

regarding Europe’s future networks. Their concerns were instrumental in developing many of the Key Findings (Section 3) and Recommendations (Section 4).

Shown below is a subset of the complete vulnerability list, indicating those vulnerabilities that the survey respondents identified as the most important. Also shown is a reference to the corresponding Recommendation(s).

Table 2: Intrinsic Vulnerabilities of Greatest Concern

POWER VULNERABILITIES	**Respondents** [%]	**Recommendations**
power limitations	**64%**	**1, 5, 10**
physical destruction	**55%**	**1, 10**
fuel dependency	**36%**	**1, 3, 5, 10**

ENVIRONMENT VULNERABILITIES	**Respondents** [%]	**Recommendations**
dependence on other infrastructures	**56%**	**1, 3, 5, 10**
remotely managed	**56%**	**1, 10**
non-compliance with established protocols and procedures	**38%**	**7, 8, 10**
exposed to elements	**38%**	**1, 10**

SOFTWARE VULNERABILITIES	**Respondents** [%]	**Recommendations**
complexity of programs	**82%**	**6, 10**
ability to control (render system in an undesirable state, confused, busy)	**45%**	**6, 10**
errors in coding logic	**45%**	**6, 10**
mutability of deployed code (patches)	**41%**	**6, 10**

HARDWARE VULNERABILITIES	**Respondents** [%]	**Recommendations**
environment (temperature, humidity, dust, sunlight, flooding)	**65%**	**1, 10**
life cycle (sparing, equipment replacement, ability to repair, aging)	**53%**	**6, 10**
electromagnetic energy (EMI, EMC, ESD, RF, EMP, HEMP, IR)	**47%**	**1, 10**

PAYLOAD VULNERABILITIES	**Respondents** [%]	**Recommendations**
authentication (mis-authentication)	**63%**	**6, 7, 8, 10**
encapsulation of malicious content	**56%**	**7, 8, 10**
insufficient inventory of critical components	**44%**	**6, 10**
encryption (prevents observability)	**44%**	**7, 8, 10**

NETWORK VULNERABILITIES	**Respondents** [%]	**Recommendations**
interconnection (interoperability, interdependence, conflict)	**68%**	**6, 8, 10**
complexity	**62%**	**8, 10**
points of concentration (congestion)	**50%**	**1, 10**

HUMAN VULNERABILITIES	**Respondents** [%]	**Recommendations**
cognitive (distractibility, forgetfulness, ability to deceive, confusion)	**67%**	**10**
ethical (divided loyalties, greed, malicious intent)	**53%**	**6, 10**
user environment (user interface, job function, corporate culture)	**40%**	**10**

POLICY VULNERABILITIES (includes Agreements, Standards, Policies and Regulations)	**Respondents** [%]	**Recommen-dations**
Interpretation of ASPR (mis- or multi-)	**50%**	**2, 7, 8, 10**
Excessive regulation	**50%**	**9, 10**
Outdated ASPR	**45%**	**2, 7, 10**
Unimplemented ASPR (complete or partial)	**45%**	**7, 8, 10**

2.5.2 Collaboration

Collaboration addresses the challenge of accelerated technology advances in that it helps bring more minds together to discuss the challenges. The methodologies used brought together industry experts to engage in ways they had never done before.

It was recognised that an approach should not shy away from the challenges associated with collaboration in the European political environment, but rather to embrace this aspect and use it as an ally. Thus, many and *different* opportunities were provided for stakeholders to provide input – from small, face-to-face meetings where information could be shared in a confidential way to protect the source, to large open workshops where experts from different types of organisations (e.g., private or public sector) could interact on the issues of most concern to them. Some industry experts that attended the workshops remarked that they had never been to such a meeting where they could interact with peers with similar expertise.[18]

The effective implementation of each of the ten Recommendations requires collaboration. From what the team observed during the Study and demonstrated with this methodology, it is confident that the kind of collaboration being called for can be achieved.

2.5.3 Confirmation of Best Practices

Another key aspect of the approach was to identify solutions that are supported with substantial buy-in from stakeholders. The identification of issues and coming to agreements on top concerns – as difficult as that can be – is not enough. These accomplishments must lead to results that can make a difference. The confirmation by European experts of industry-consensus Best Practices is an example of such progress, and represents a milestone in improving the reliability of European networks.

Overview of the European Experts Survey
As part of the Study, a survey was completed by a diverse set of stakeholders representing multiple industries, network types, and academia. The survey was divided into three parts:

1. Top concerns related to future networks
2. Vulnerability concerns for future networks
3. Best Practice effectiveness survey for future networks

[18] "These ground breaking workshops are bringing together experts for rigorous discussions on Europe's future communications networks. . . . These workshops are a necessary role model for achieving consensus for Europe's ICT community. I am certain that the output of these workshops will provide bold, actionable and much needed guidance . . . " Franchina, L., Director General, Italian Ministry of Communications, (www.comsoc.org/~cqr/EU-Proceedings-2006).

The top concerns identified in the survey were discussed at four European experts workshops,[19] jointly sponsored by the IEEE Communications Society Technical Committee on Communications Quality & Reliability (CQR) and Bell Labs. Each event was hosted by a significant European stakeholder at each location. The output of these workshops was a major basis for the Key Findings and Recommendations made in this Study.

European Experts Workshops

- Power & Environment – 3 October 2006 – *Rome, Italy*
  Hosted by Italian Ministry of Communications
- Network & Payload – 6 October 2006 – *London, England*
  Hosted by BT
- Hardware & Software – 11 October 2006 – *Berlin, Germany*
  Hosted by Rohde & Schwarz SIT
- Policy & Human – 15 November 2006 – *Brussels, Belgium*
  Hosted by SWIFT (Society for Worldwide Interbank Financial Telecommunication)

The second section of the survey asked stakeholders to identify their top vulnerability concerns for future networks from a list of vulnerabilities associated with each of the eight ingredients. The results of this selection are detailed in Section 2.5.1.

The survey concluded by asking the stakeholders to evaluate a list of industry Best Practices.[20] Stakeholders were asked to evaluate Best Practices in their areas of expertise relative to the eight ingredients (e.g., hardware, networks, power, policy). The experts rated each Best Practice in terms of four dimensions: “Effectiveness”, “Cost to Implement”, “Risk to *Not* Implement”, and “Level of Implementation”. The results of the experts’ evaluation were used to establish a set of Best Practices relevant for European telecommunication space.

Effectiveness

Best Practice Selection Criteria

Best Practice receiving a positive “Effectiveness” rating (either effective or moderately effective) from at least 90% of the experts were included in the following Best Practice list. Best Practices that were evaluated by only a small number of experts were not included. Based on the analysis criteria, a total of 71 Best Practices have been identified. This list will serve as the basis for further European Best Practice collaboration. They can be accessed online at www.bell-labs.com/EUROPE/bestpractices/ .

The confirmed Best Practices and their associated unique identifiers[21] are provided below, sorted based on the eight ingredients.[22]

[19] The proceedings for the four workshops can be found at www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[20] These best practices were previously developed by global communications companies and have been shown to be beneficial to European network operators and equipment suppliers.

[21] Best Practice EU06-5204 can be referred to as BP 5204. The EU06 is used to track when the Best Practice was last modified.

[22] Best Practices for six of the eight ingredients have been defined. Two of the ingredients (Environment, Human) received insufficient votes to be statistically significant, and therefore no European Best Practices have as yet been identified for these two ingredients.

POWER BEST PRACTICES

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should develop documentation for the restoration of power for areas of critical infrastructure including such things as contact information, escalation procedures, restoration steps and alternate means of communication. This documentation should be maintained both on-site and at centralised control centres. EU06-5231

- Network Operators should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with the site specific constraints, criticality of the site, the expected load and reliability of primary power. EU06-0492

- Network Operators, Service Providers and Property Managers should place strong emphasis on human activities related to the operation of power systems (e.g., maintenance procedures, alarm system operation, response procedures, and training) for operations personnel. EU06-0650

- Network Operators, Service Providers and Property Managers should design standby generator systems for fully automatic operation and for ease of manual operation, when required. EU06-0657

- Network Operators, Service Providers and Property Managers should exercise power generators on a routine schedule in accordance with manufacturer's specifications. For example, a monthly 1 hour engine run on load, and a 5 hour annual run. EU06-0662

- Network Operators, Service Providers and Property Managers should develop and test plans to address situations where normal power backup does not work (e.g., commercial AC power fails, the standby generator fails to start, automatic transfer switch fails). EU06-0695

- Network Operators, Service Providers and Property Managers should perform annual capacity evaluation of power equipment, and perform periodic scheduled maintenance, including power alarm testing. EU06-0773

- Network Operators and Service Providers should periodically review their portable power generator needs to address changes to the business. EU06-1029

- Service Providers, Network Operators and Property Managers should ensure availability of emergency/backup power (e.g., batteries, generators, fuel cells) to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown/black outs, terrorism). The emergency/backup power generators should be located onsite, when appropriate. EU06-5204

- Network Operators, Service Providers and Property Managers should maintain sufficient fuel supplies for emergency/backup power generators running at full load to allow for contracted refuelling. EU06-5206

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that electrical work (e.g., AC and high current DC power distribution) is performed by qualified technicians. EU06-5208

- Network Operators, Service Providers and Property Managers should consider placing generator sets and fuel supplies for critical sites within a secured area to prevent unauthorised access, reduce the likelihood of damage and/or theft, and to provide protection from explosions and weather. EU06-5212

- Network Operators, Service Providers and Property Managers should, where feasible, place fuel tanks in a secured and protected area. Access to fill pipes, fuel lines, vents, manways, etc. should be restricted (e.g., containment by fencing, walls, buildings, buried) to reduce the possibility of unauthorised access. EU06-5213

- Network Operators, Service Providers, and Property Managers should test fuel reserves used for standby or backup power for contamination at least once a year or after any event (e.g., earth tremor, flood) that could compromise the integrity of the tank housing, fill pipe or supply pipe. EU06-5232

HARDWARE BEST PRACTICES

- Software & Hardware Vulnerability Tracking: Service Providers should monitor software and hardware vulnerability reports and take the recommended action(s) to address problems, where appropriate. These reports and recommendations are typically provided by equipment suppliers and CERTs (Computer Emergency Response Teams). EU06-0428

- Equipment Suppliers should design outdoor equipment (e.g., base station) to operate in expected environmental conditions (e.g., weather, earthquakes). EU06-0459

- Equipment Identification: Network Operators, Service Providers and Equipment Suppliers should position the equipment designation information (e.g., location, labels, RFID tags) so that they are securely affixed. The equipment designation should not be placed on removable parts such as covers, panels, doors, or vents that can be removed and mistakenly installed on a different network element. EU06-0614

- Network Operators, Service Providers and Equipment Suppliers should maintain the availability of spares for critical network systems. EU06-5083

- Equipment Suppliers of critical network elements should test electronic hardware to ensure its compliance with design criteria for tolerance to electromagnetic energy, shock, vibration, voltage spikes, and temperature. EU06-5118

- Network Operators, Service Providers and Equipment Suppliers should establish and implement procedures for the proper disposal and/or destruction of hardware (e.g., hard drives) that contain sensitive or proprietary information. EU06-5200

- Equipment Suppliers should provide network element thermal specifications or other special requirements in order to properly size Heating, Ventilation, and Air Conditioning (HVAC) systems. EU06-5283

SOFTWARE BEST PRACTICES

- Software Configurations: Equipment Suppliers should be able to recreate supported software from source and, where feasible, software obtained from third parties. EU06-0430

- Network Operators, Service Providers and Equipment Suppliers should develop and consistently implement software delivery procedures that protect the integrity of the delivered software in order to prevent software loads from being compromised during the delivery process. EU06-5121

- Expedited Security Patching: Network Operators, Service Providers and Equipment Suppliers should have special processes and tools in place to quickly patch critical infrastructure systems when important security patches are made available. Such processes should include determination of when expedited patching is appropriate and identifying the organisational authority to proceed with expedited patching. This should include expedited lab testing of the patches and their affect on network and component devices. EU06-8020

- Software Patching Policy: Network Operators and Service Providers should define and incorporate a formal patch/fix policy into the organisation's security policies. EU06-8034

- Software Patch Testing: The patch/fix policy and process used by Network Operators and Service Providers should include steps to appropriately test all patches/fixes in a test environment prior to distribution into the production environment. EU06-8035

NETWORK BEST PRACTICES

- Network Surveillance: Network Operators and Service Providers should monitor their networks to enable quick response to network issues. EU06-0401

- Network Performance: Network Operators and Service Providers should periodically examine and review their networks to ensure that it meets the current design specifications. EU06-0405

- NOC Communications: Network Operators and Service Providers should establish processes for NOC-to-NOC (Network Operations Centre) peer communications for critical network activities (e.g., scheduled maintenance, upgrades and outages). EU06-0407

- Data Back-up Verification: Network Operators and Service Providers should test the restoral process associated with critical data back-up, as appropriate. The goal is to demonstrate that data restoration is complete and works as expected. EU06-0415

- Network Operators and Service Providers should report problems discovered from their operation of network equipment to the Equipment Supplier whose equipment was found to be the cause of problem. EU06-0501

- Network Operators, Service Providers and Equipment Suppliers should, by design and practice, manage critical Network Elements (e.g., Domain Name Servers, Signalling Servers) that are essential for network connectivity and subscriber service as critical systems (e.g., secure, redundant, alternative routing). EU06-0510

- Network Operators and Service Providers should maintain a "24 hours by 7 days" contact list of other providers and operators for service restoration of inter-connected networks. Where appropriate, this information should be shared with Public Safety Service and Support providers. EU06-0513

- Diversity Audit: Network Operators should periodically audit the physical and logical diversity called for by network design and take appropriate measures as needed. EU06-0532

- Network Operators and Service Providers should minimise single points of failure (SPOF) in paths linking network elements deemed critical to the operations of a network (with this design, two or more simultaneous failures or errors need to occur at the same time to cause a service interruption). EU06-0546

- Network Operators, Service Providers and Equipment Suppliers should prepare Methods of Procedure (MOPs) for core infrastructure hardware and software growth and change activities as appropriate. EU06-0590

- Network Operators and Service Providers should be aware of the dynamic nature of peak traffic periods and should consider scheduling potentially service-affecting procedures (e.g., maintenance, high risk procedures, growth activities) so as to minimise the impact on end-user services. EU06-0595

- Network Operators and Service Providers should conduct exercises periodically to test a network's operational readiness through planned drills or simulated exercises. The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible. EU06-0599

- Network Operators and Service Providers should establish and document a process to plan, test, evaluate and implement major change activities onto their network. EU06-0600

- Schedule System Backups: Network Operators and Service Providers should establish policies and procedures that outline how critical network element databases will be backed up onto a storage medium (e.g., tapes, optical diskettes) on a scheduled basis. EU06-0603

- Network Operators and Service Providers should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network, before it is placed into service. EU06-0612

- Network Operators and Service Providers should develop and implement defined procedures for removal of unused equipment and cable (e.g., cable mining) if this work can be economically justified without disrupting existing service. EU06-0628

- Network Operators should provide physical diversity on critical inter-office routes when justified by a risk or value analysis. EU06-0731

- Network Operators and Service Providers should conduct periodic verification of the office synchronisation plan and the diversity of timing links, power feeds and alarms. EU06-0761

- Network Diversity: Network Operators and Service Providers should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path). EU06-5075

PAYLOAD BEST PRACTCIES

- Network Operators and Service Providers should, where feasible, deploy SPAM controls in relevant nodes (e.g., message centres, email gateways) in order to protect critical network elements and services. EU06-0449

- Attack Trace Back: Network Operators, Service Providers and Equipment Suppliers should have the processes and/or capabilities to analyze and determine the source of malicious traffic, and then to trace-back and drop the packets at, or closer to, the source. The references provide several different possible techniques. (Malicious traffic is that traffic such as Distributed Denial of Service (DDoS) attacks, smurf and fraggle attacks, designed and transmitted for the purpose of consuming resources of a destination of network to block service or consume resources to overflow state that might cause system crashes). EU06-0507

- Network Operators and Service Providers should have a route policy that is available, as appropriate. A consistent route policy facilitates network stability and inter-network troubleshooting. EU06-0520

- Service Providers, Network Operators and Equipment Suppliers should work to establish operational standards and practices that support broadband capabilities and interoperability (e.g., video, voice, data, wireless). EU06-0805

- For the deployment of Residential Internet Access Service, Broadband Network Operators should design in the ability to take active measures to detect and restrict or inhibit any network activity that adversely impacts performance, security, or usage policy. EU06-0814

- For the deployment of Residential Internet Access Service, a Broadband Network Operator should incorporate multilevel security schemes for network data integrity, as applicable, in the network design to prevent user traffic from interfering with network operations, administration, and management use. EU06-0822

- Network Operators, Service Providers and Equipment Suppliers should, where feasible, ensure that intentional emissions (e.g., RF and optical) from network equipment and transmission facilities are secured sufficiently to ensure that monitoring from outside the intended transmission path or beyond facility physical security boundaries cannot lead to the obtaining of critical network operations information. EU06-5149

- Define Security Architecture(s): Network Operators and Service Providers should develop formal written Security Architecture(s) and make the architecture(s) readily accessible to systems administrators and security staff for use during threat response. The Security Architecture(s) should anticipate and be conducive to business continuity plans. EU06-8007

- Network Architecture Isolation/Partitioning: Network Operators and Service Providers should implement architectures that partition or segment networks and applications using means such as firewalls, demilitarized zones (DMZ), or virtual private networks (VPN) so that contamination or damage to one asset does not disrupt or destroy other assets. In particular, where feasible, it is suggested the user traffic networks, network management infrastructure networks, customer transaction system networks, and enterprise communication/business operations networks be separated and partitioned from one another. EU06-8008

- Operational Voice over IP (VoIP) Server Hardening: Network Operators should ensure that network servers have authentication, integrity, and authorisation to prevent inappropriate use of the servers. Enable logging to detect inappropriate use. EU06-8056

- Intrusion Detection/Prevention (IDS/IPS) Tools Deployment: Network Operators and Service Providers should deploy Intrusion Detection/Prevention Tools with an initial policy that reflects the universe of devices and services known to exist on the monitored network. Due to the ever evolving nature of threats, IDS/IPS tools should be tested regularly and tuned to deliver optimum performance and reduce false positives. EU06-8073

- Adopt and Enforce Acceptable Use Policy: Network Operators and Service Providers should adopt a customer-directed policy whereby misuse of the network would lead to measured enforcement actions up to and including termination of services. EU06-8092

- Protect Sensitive Data in Transit for Externally Accessible Applications: Network Operators and Service Providers should encrypt sensitive data from web servers, and other externally accessible applications, while it is in transit over any networks they do not physically control. EU06-8111

POLICY BEST PRACTICES

- Network Operators and Service Providers should have procedures in place to process court orders and subpoenas for wire taps or other information. EU06-0505

- Network Operators and Service Providers should establish company-specific interconnection agreements, and where appropriate, utilise existing interconnection templates and existing data connection trust agreement. EU06-0508

- Network Operators, Service Providers and Equipment Suppliers are encouraged to continue to participate in the development and expansion of industry standards for traffic management that promote interoperability and assist in meeting end-user quality of service needs. EU06-0803

- Network Operators and Service Providers should document their critical equipment suppliers, vendors, contractors and business partners in their Business Continuity Plans along with an assessment of the services, support, and capabilities available in the event of a disaster. EU06-1032

- Network Operators, Service Providers and Equipment Suppliers should work collectively with regional, and national governments as well as European agencies to develop relationships fostering efficient communications, coordination and support for emergency response and restoration. EU06-1058

- Network Operators, Service Providers and Equipment Suppliers should consider establishment of a senior management function for a chief security officer (CSO) or functional equivalent to direct and manage both physical and cyber security. EU06-5070

- In order to prepare for contingencies, Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department and other security and emergency agencies to exchange critical information related to threats, warnings and mutual concerns. EU06-5071

- Network Operators, Service Providers and Equipment Suppliers should interact as needed with regional, and national governments as well as European agencies to identify and address potential adverse security impacts of new laws and regulations (e.g., exposing vulnerability information, required security measures, fire codes). EU06-5100

- Network Operators should not share information pertaining to the criticality of individual communication facilities or the traffic they carry, except with trusted entities for justified specific purposes with appropriate protections against further disclosure. EU06-5110

- Network Operators, Service Providers and Equipment Suppliers should, at the time of the event, coordinate with the appropriate regional, and national governments as well as European agencies to facilitate timely access by their personnel to establish, restore or maintain communications, through any governmental security perimeters (e.g., civil disorder, crime scene, disaster area). EU06-5112

- Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department, other utilities and other security and emergency agencies to ensure effective coordination for emergency response and restoration. EU06-5226

- Network Operators', Service Providers', Equipment Suppliers' and Property Managers' senior management should actively support compliance with established corporate security policies and procedures. EU06-5265

- Sharing Information with Law Enforcement: Network Operators, Service Providers and Equipment Suppliers should establish a process for releasing information to members of the law enforcement and intelligence communities and identify a single Point of Contact (POC) for coordination/referral activities. EU06-8065

Cost and Risk

Because implementation of Best Practices is voluntary, both the *cost of implementing* them and the *risk of **not** implementing* them need to be considered. A total of 900 opinions from industry experts, spread across the 71 identified Best Practices, were analyzed to address these issues. Shown below are charts representative of the type of analysis that was conducted for each of the eight ingredients.

Cost to Implement

71% of the total responses indicate that the cost to implement the Best Practices is either low or moderate. This indicates that voluntary implementation of Best Practices is feasible, but certainly not free. Each organisation must decide for itself where to implement and where not to implement specific Best Practices in their networks or products.

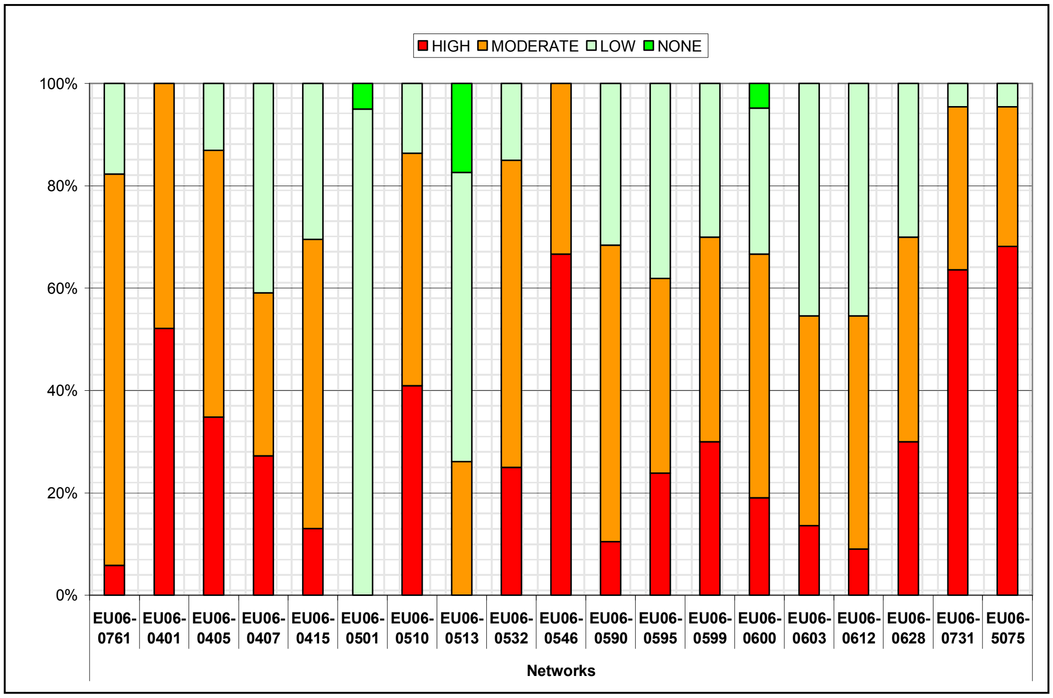


Figure 4: Example - Analysis of Cost to Implement

Risk to Not Implement

91% of the total responses indicate that the risk to ***not*** implement the Best Practices is either high or moderate. 27 of the 71 Best Practices had no instances where any of the experts considered the "risk of not implementing" as being "low". This shows the incentive to implement Best Practices in critical networks or products, and gives a clear indication that the industry experts believe these Best Practices provide solutions to real concerns.

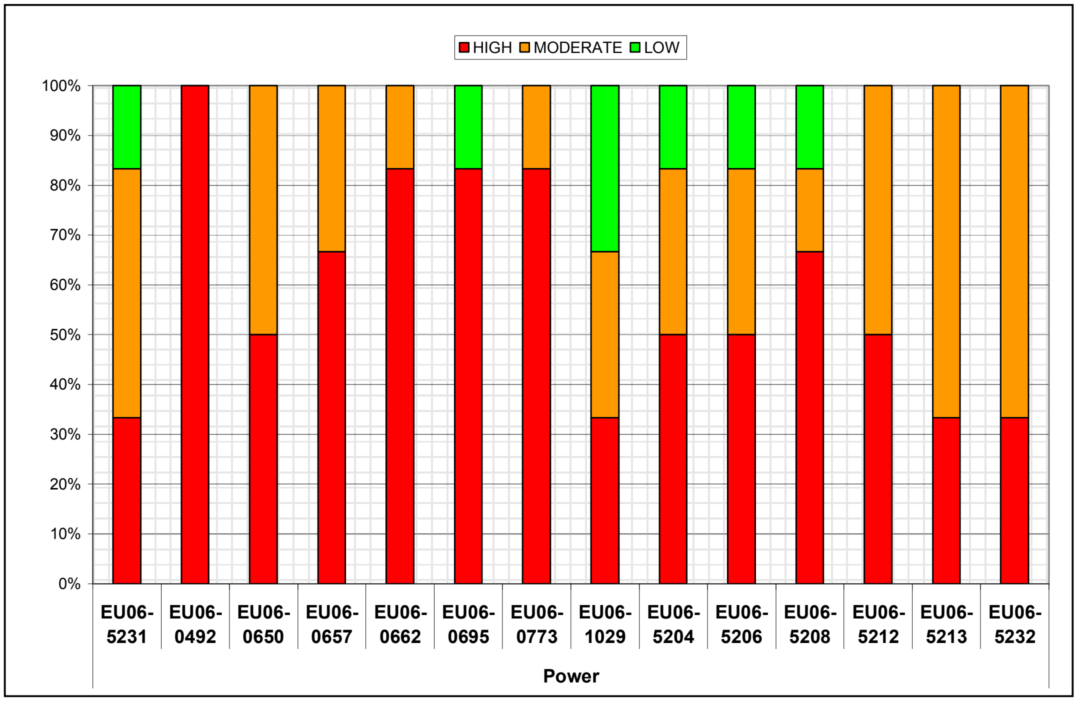


Figure 5: Example – Analysis of Risk to NOT Implement

Level of Implementation

The level of implementation of the Best Practices was very high. 94% of the total responses indicate that the specific Best Practices are implemented "everywhere" or "everywhere critical" in the experts' networks or products. 70 of 71 Best Practices were identified as being implemented everywhere or everywhere critical by at least 80% of the experts. Further, 32 of the 71 Best Practices had *no* instances of "not implemented". This is a clear indication that the Best Practices have value. It can also be inferred that while there are costs associated with implementing these Best Practices, a significant part of those costs have already been incurred.

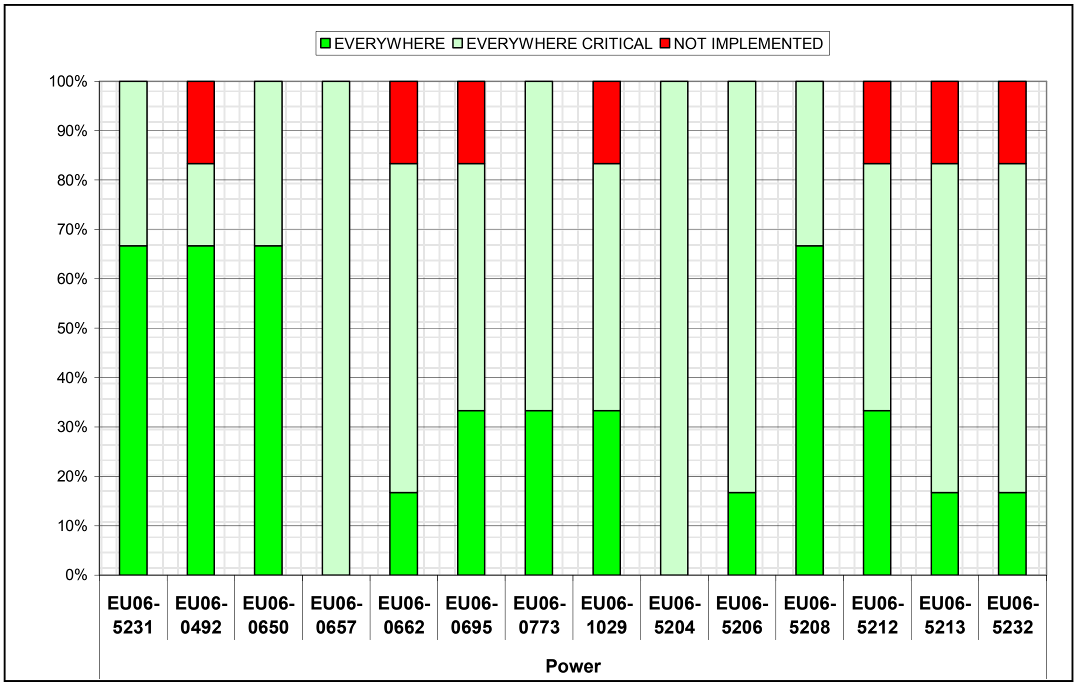


Figure 6: Example – Analysis of Level of Implementation

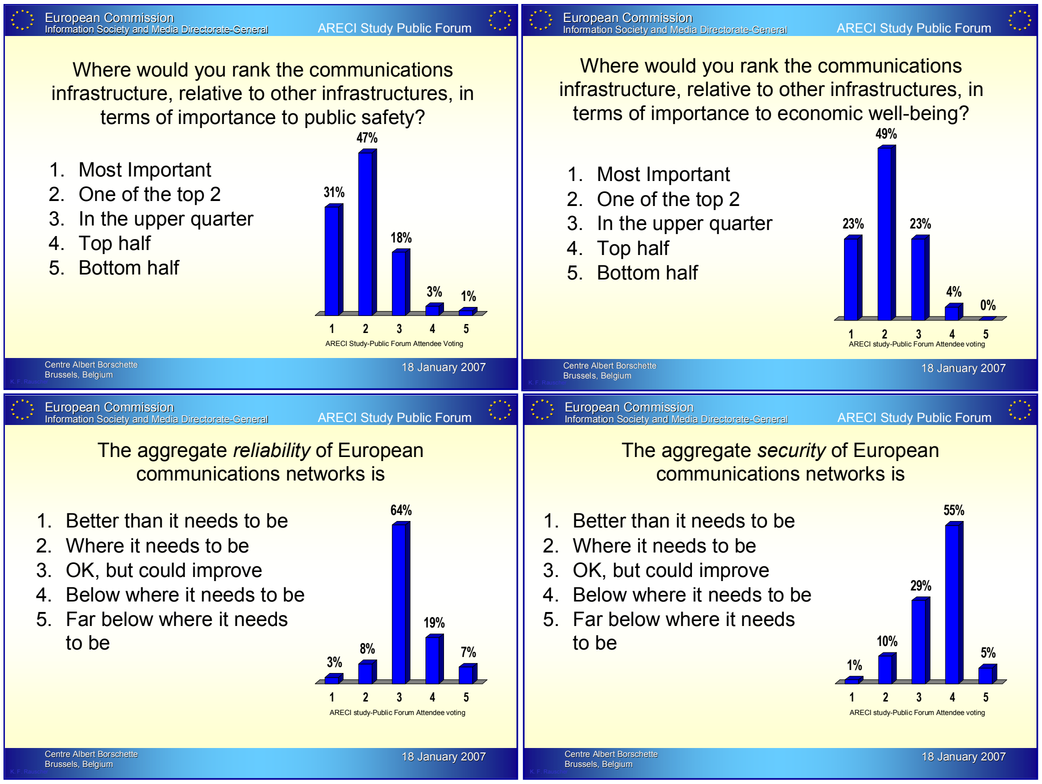
2.5.4 Public Forum

On January 18th 2007 the European Commission hosted the "ARECI Public Forum" in Brussels. The event was held at the Centre Albert Borschette and was directly supported by European Commission leaders.[23]

The event was designed to present the findings of the ARECI report to Europe's communications experts and to gather their feedback on the Study's ten Recommendations. Over 100 stakeholders representing industry, academia, research and Member States participated in the Forum. Four guest speakers opened the Forum by providing their perspectives on the importance of communications for their sectors.[24]

A real-time voting system was employed during the Forum to collect immediate feedback from participants. The voting was divided into three parts. The first part looked at the criticality of communications and where networks currently stand in terms of reliability and security. 90% of the participants indicated that both reliability and security of communications networks should be improved, and 78% identified communications as one of the two most critical infrastructures.

[23] Fabio Colasanti, Director General, Information Society and Media; Andrea Servida, Deputy Head of Unit, Internet, Network and Information Security; Magnus Ovilius, chef de secteur, Directorate General Justice Liberty and Security.
[24] Christian Grégoire, CTO, Alcatel-Lucent Europe; Stephen Malphrus, chief of staff, U.S. Federal Reserve Board; Didier Verstichel, director, Enterprise Security & Architecture, SWIFT; Tony Burgon, network manager, DHL Europe.



European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

Where would you rank the communications infrastructure, relative to other infrastructures, in terms of importance to public safety?

1. Most Important
2. One of the top 2
3. In the upper quarter
4. Top half
5. Bottom half

ARECI Study-Public Forum Attendee Voting

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

Where would you rank the communications infrastructure, relative to other infrastructures, in terms of importance to economic well-being?

1. Most Important
2. One of the top 2
3. In the upper quarter
4. Top half
5. Bottom half

ARECI study-Public Forum Attendee voting

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

The aggregate *reliability* of European communications networks is

1. Better than it needs to be
2. Where it needs to be
3. OK, but could improve
4. Below where it needs to be
5. Far below where it needs to be

ARECI study-Public Forum Attendee voting

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

The aggregate *security* of European communications networks is

1. Better than it needs to be
2. Where it needs to be
3. OK, but could improve
4. Below where it needs to be
5. Far below where it needs to be

ARECI study-Public Forum Attendee voting

Centre Albert Borschette
Brussels, Belgium
18 January 2007

Figure 7: Public Forum Stakeholder Voting on Communications Infrastructure

The second set of voting questions came after the ten Recommendations were presented, and asked the participants whether each Recommendation was worth considering for implementation. Shown below are the percentages of participants who voted "**Agree**" and "**Strongly Agree**" for each Recommendation.

95% for Recommendation 1, **EMERGENCY PREPAREDNESS**

87% for Recommendation 2, **PRIORITY COMMUNICATIONS**

88% for Recommendation 3, **MUTUAL AID**

81% for Recommendation 4, **INFORMATION SHARING**

92% for Recommendation 5, **INFRASTRUCTURE INTERDEPENDENCIES**

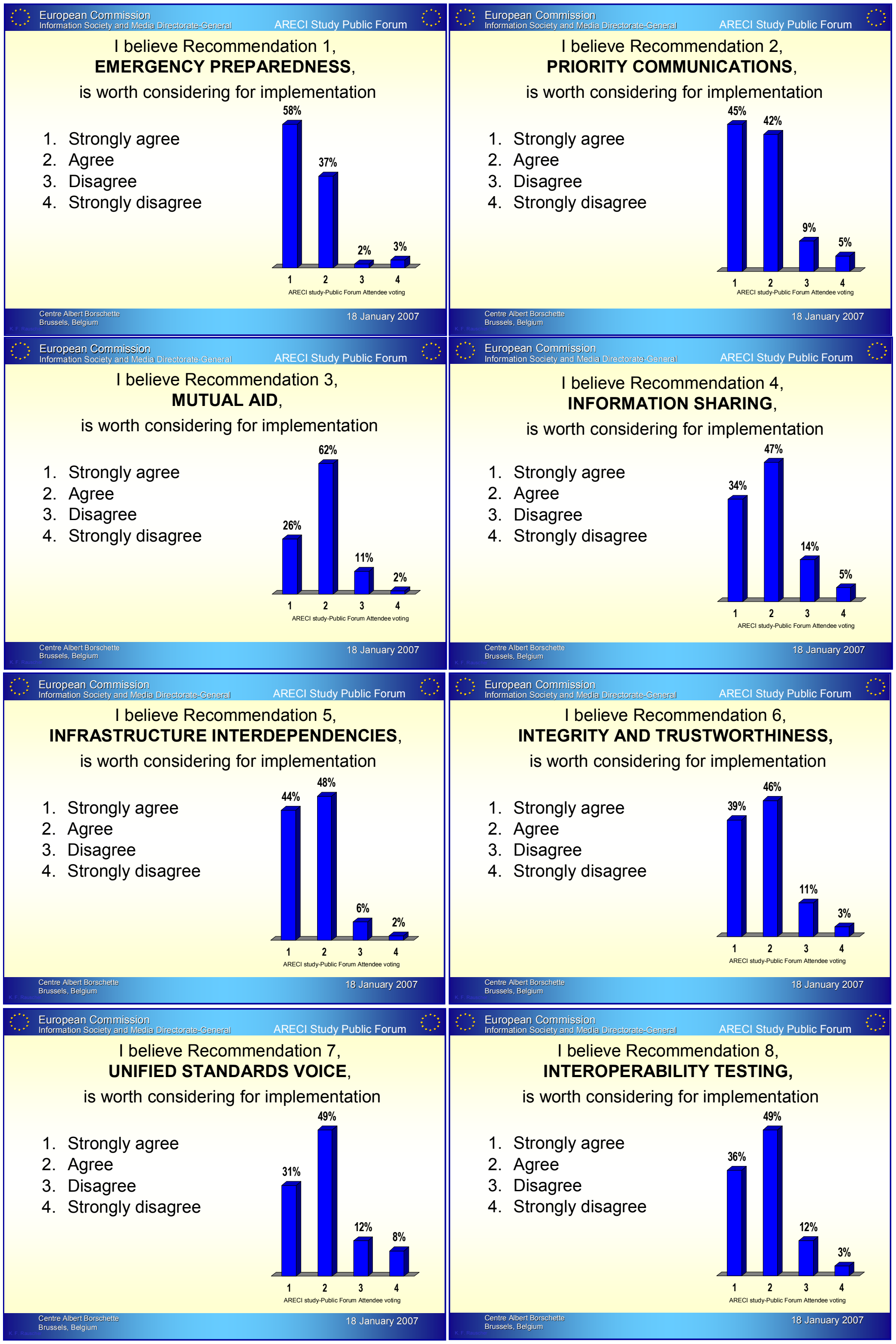
85% for Recommendation 6, **INTEGRITY AND TRUSTWORTHINESS**

80% for Recommendation 7, **UNIFIED STANDARDS VOICE**

85% for Recommendation 8, **INTEROPERABILITY TESTING**

77% for Recommendation 9, **PARTNERSHIP HEALTH OWNERSHIP**

91% for Recommendation 10, **DISCRETIONARY BEST PRACTICES**



European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe Recommendation 1,
EMERGENCY PREPAREDNESS,
is worth considering for implementation

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe Recommendation 2,
PRIORITY COMMUNICATIONS,
is worth considering for implementation

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe Recommendation 3,
MUTUAL AID,
is worth considering for implementation

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe Recommendation 4,
INFORMATION SHARING,
is worth considering for implementation

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe Recommendation 5,
INFRASTRUCTURE INTERDEPENDENCIES,
is worth considering for implementation

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe Recommendation 6,
INTEGRITY AND TRUSTWORTHINESS,
is worth considering for implementation

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe Recommendation 7,
UNIFIED STANDARDS VOICE,
is worth considering for implementation

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

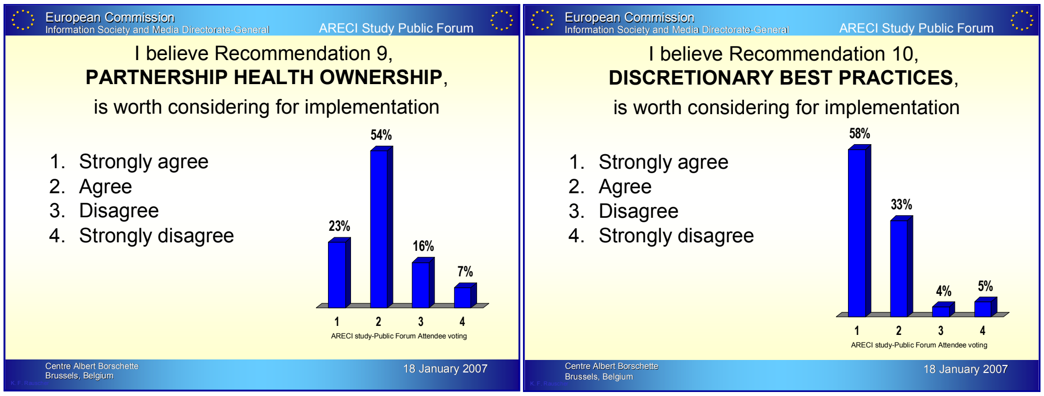
European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe Recommendation 8,
INTEROPERABILITY TESTING,
is worth considering for implementation

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

Figure 8: Public Forum Stakeholder Voting on Recommendations



European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe Recommendation 9,
PARTNERSHIP HEALTH OWNERSHIP,
is worth considering for implementation

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

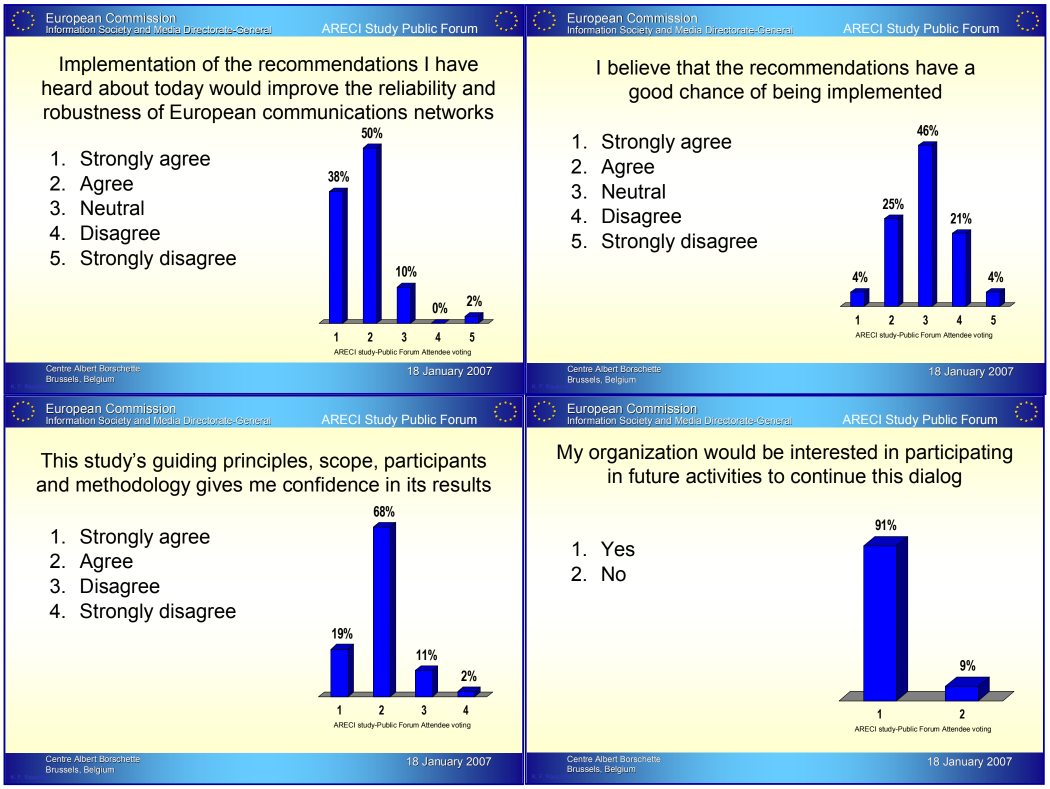
European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe Recommendation 10,
DISCRETIONARY BEST PRACTICES,
is worth considering for implementation

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

Figure 8: Public Forum Stakeholder Voting on Recommendations (continued)



European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

Implementation of the recommendations I have heard about today would improve the reliability and robustness of European communications networks

1. Strongly agree
2. Agree
3. Neutral
4. Disagree
5. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

I believe that the recommendations have a good chance of being implemented

1. Strongly agree
2. Agree
3. Neutral
4. Disagree
5. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

This study's guiding principles, scope, participants and methodology gives me confidence in its results

1. Strongly agree
2. Agree
3. Disagree
4. Strongly disagree

Centre Albert Borschette
Brussels, Belgium
18 January 2007

European Commission
Information Society and Media Directorate-General
ARECI Study Public Forum

My organization would be interested in participating in future activities to continue this dialog

1. Yes
2. No

Centre Albert Borschette
Brussels, Belgium
18 January 2007

Figure 9: Public Forum Stakeholder Summary Voting

The final set of questions related to the ARECI report as a whole. 88% of the participants either **strongly agreed** or **agreed** that implementation of the ten Recommendations would improve the reliability and robustness of European networks, however only 29% **strongly agreed** or **agreed** that the Recommendations have a good chance of being implemented. Reasons given for the difficulty to implement included "the funding won't be available" (13%), "government isn't ready for this (22%), and "neither industry or government is ready for this (48%). This is a clear indication that while there is definitely value in implementing the Recommendations, there will be obstacles to overcome to achieve the desired improvements. It was encouraging that 91% of the participants indicated that their organisation would be interested in participating in future activities to continue the dialog.[25]

2.6 Recommendation Development

The final component of the methodology was the thorough review of well over 30,000 data points. A three step process was used to arrive at the Recommendations made in this report. Ideas were generated based on European perspectives and collected data. These ideas were then compared against trends and experiences seen in other parts of the world and Recommendations were developed. These Recommendations were then validated from multiple perspectives to ensure their applicability to a broad range of stakeholders.

A value-adding feature of the Recommendation development was the inclusion of several elements that do not always accompany such guidance. The first of these is a concise statement of alternatives to the guidance being made. Each alternative is followed by the Study team's anticipated outcome of following that course of action. The second component is a set of suggested next steps. A complete plan is not offered, but rather some clear actions that carry on the momentum generated during the Study. The third element is a list of measures of success. Articulating such parameters assists not only in making the guidance more achievable, but also makes it clearer.

In summary, the methodology used throughout the Study is based on proven approaches for similar highly consequential advisory undertakings regarding critical infrastructure. The framework, range of experience and expertise, personal interaction and recommendation process enabled the Study team to delve deeply into the issues facing Europe's future networks, draw upon the knowledge of those most familiar with it, and establish a model for future interaction and sharing.

[25] More information on the Public Forum can be found at www.bell-labs.com/ARECI

3 KEY FINDINGS

The purpose of study is learning. In order to make recommendations on improving the reliability and robustness of future networks, the team of experts assembled to conduct this Study needed to learn about present conditions in Europe relative to current networks and plans for future networks. This was accomplished primarily by three methods: face-to-face interviews with experts from industry, academia, and government; analysis of virtual interviews conducted with a wide range of stakeholders; and four day-long experts workshops, each of which focused on two of the eight communications infrastructure ingredients. As described in Section 2.4, these sources are representative of the evolving European communications landscape. The learnings from these efforts, combined with the experience and knowledge of the Study team, yielded the following 100 Key Findings. The Key Findings reflect the sometimes dissimilar views of the various stakeholders, combined and tempered by the perspective of the expert Study team.

In this section, the Key Findings are presented in the context of the Availability and Robustness Maturity Model (Figure 7).[26] The Availability and Robustness Maturity Model uses a five level categorisation structure that associates a level of sophistication with each observation. During this Study, the members of the Study team associated their Key Findings with one of five levels. The maturity level association was made based on the Study team's familiarity with benchmarks of operations as described below. In practice, most operations will find that they can identify with Key Findings categorised in an assortment of maturity levels. A description of each maturity level can be found at the beginning of each section. There are many ways to organise these findings, and the Study team considered carefully which would be most appropriate. In the end, the Availability and Robustness Maturity Model was selected, as it was determined to provide the most value to the audience by conveying the combined expertise of the Study team. In addition, the model also reflects the responses, including nonverbal, of the stakeholders involved in the Study. Here is a summary of the five levels:

Novice Level (1) observations are representative of an operation that is just entering the communications industry. This category includes common sense items and the most fundamental aspects of support for services.

Basic Level (2) observations are representative of an operation that is commonly recognised as part of the communications industry, but is still working on implementing practices and procedures to consistently address routine occurrences in their network.

Common Level (3) observations are representative of a well established operation in the communications industry. This level includes items that incumbent operators usually have addressed, but newer entrants may be still working to implement.

Advanced Level (4) observations are representative of an operation that has begun implementing new strategies to deal with the nuances associated with interfacing future networks with legacy networks.

[26] Annex A organises the same Key Findings using the Eight Ingredient Framework structure.

This level includes items to address the realities of changing threats to critical infrastructure and working cooperatively with other organisations in the industry.

State-of-the-Art Level (5) observations are representative of an operation that has embraced the challenges of future networks and is leading the way in addressing those challenges. This category includes inventing and implementing policies for which there may be no current standard and looking beyond themselves to the industry as a whole.

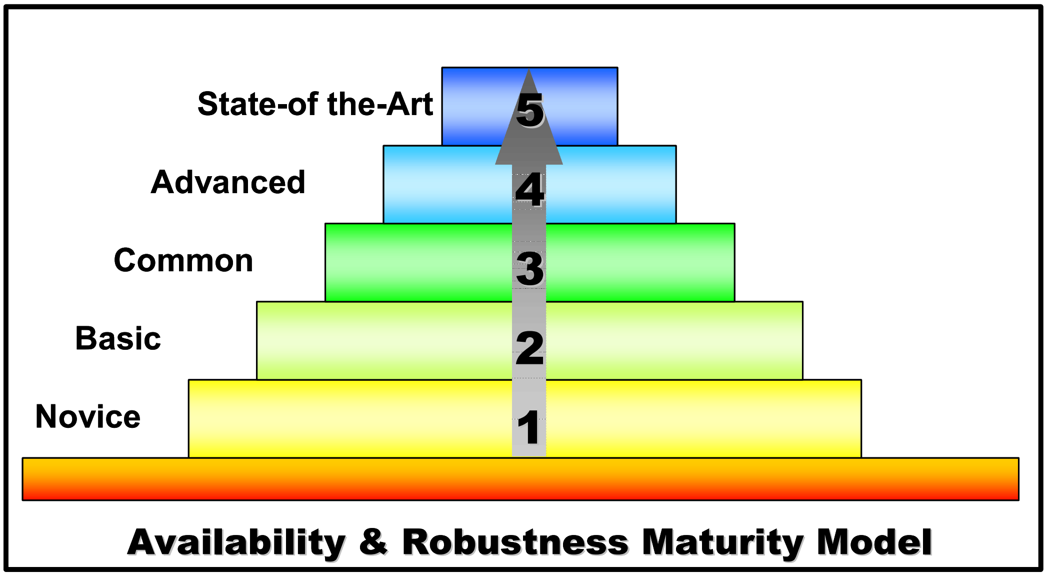


Figure 10: Availability and Robustness Maturity Model

Any of these observations may apply to an organisation regardless of the overall maturity level of that organisation. As such, each organisation should carefully consider each of the 100 observations listed in this section.

For those interested in certain areas, each Key Finding is presented here with one or more of the eight ingredients[27] with which it is directly associated (Figure 2). For example, if a Key Finding is an observation primarily with software and hardware, then one pink (🟪 software) and one blue (🟦 hardware) squares are indicated in the right hand margin. The widely varying array of ingredient indicators in the right column expresses the complex interactions of the disciplines that are needed to support communications infrastructure. Annex B also provides a relationship between the complete list of Key Findings and the eight ingredients.

[27] *Scope*, Section 2.2.

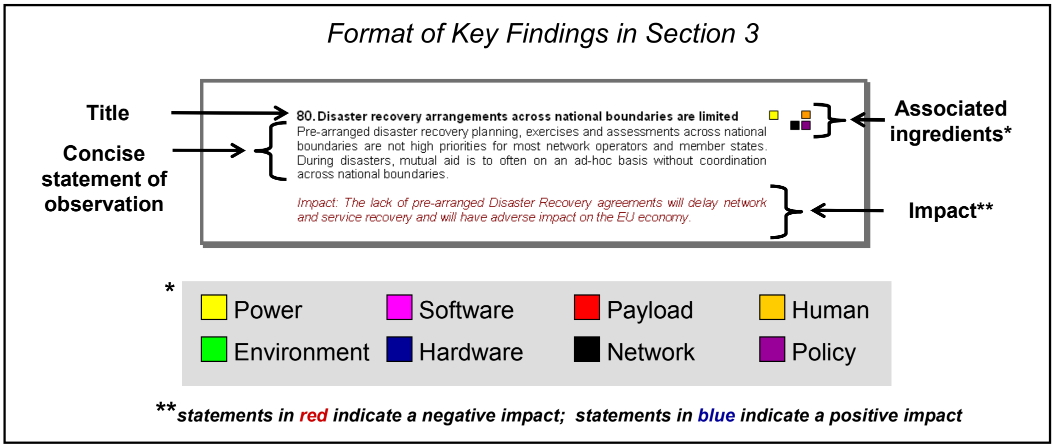

Format of Key Findings in Section 3
Title
Concise statement of observation
80. Disaster recovery arrangements across national boundaries are limited
Pre-arranged disaster recovery planning, exercises and assessments across national boundaries are not high priorities for most network operators and member states. During disasters, mutual aid is to often on an ad-hoc basis without coordination across national boundaries.
Impact: The lack of pre-arranged Disaster Recovery agreements will delay network and service recovery and will have adverse impact on the EU economy.
Associated ingredients*
Impact**
*
Power
Software
Payload
Human
Environment
Hardware
Network
Policy
**statements in red indicate a negative impact; statements in blue indicate a positive impact

Figure 11: Presentation of Key Findings

3.1 Novice Level Observations - Maturity Level 1

The five observations presented here are representative of an operation that is just entering the communications industry or is just establishing itself. Such organisations are often developing policies and procedures on the fly, and while they may be experienced with their particular product or service, may not have much general business experience or experience in the industry they're entering. Details of establishing the business and day-to-day operation often take precedence over longer term planning and preparation. This category includes common sense items and the most fundamental aspects of support for services.

1. Some government leaders have the mindset of "It can't happen here" 🟨 🟧 ⬛

There is variation regarding the recognition by government leaders that a catastrophic event can occur in their country. Of concern is that some of the countries that have not experienced a recent disaster have a *low expectation* that one can occur in the future, and thus they do not plan nor invest for dealing with such a crisis.

Impact: Because EU Member States have significant critical sector dependencies on electronic communications infrastructures, a major disaster could have a more severe negative impact than for a country in an earlier stage of economic development.

2. Location issues associated with public-to-authority VoIP calls are unresolved[28] 🟥 ⬛

As future networks service providers process public-to-authority emergency calls (e.g., 112 calls), they will face the still unresolved issues regarding VoIP nomadicity. The network-derived caller's location information may be absent or, worse, incorrect.

[28] This finding does not address the emergency services infrastructure, but rather the fact that VoIP calls are occurring everywhere where there is Internet assess and interconnection to the PSTN. Subscribers can be told by operators not to call emergency numbers from their VoIP phones, but subscribers could ignore the prohibition or the VoIP phone is the only phone that one has during an emergency. According to our observations there are EU citizens having only VoIP subscription for cost reasons. The IETF ECRIT WG is currently addressing this with strong interest from many parties and where a stronger EU presence would be useful. There is the very real risk that by the time a decision is made, the standards may already be completed and not have benefited from EU input.

Many service providers may not offer end-to-end emergency call service or may not treat these calls differently from ordinary calls.

Impact: Subscribers on future networks may not have a reliable means for placing emergency calls in all circumstances.

3. Emergency preparedness is largely informal 🟨 🟩 ⬛

Service providers and network operators may depend upon informal and ad hoc responses to emergencies. This tendency is notably more common among newer market entrants.

Impact: While emergencies always require some flexibility, a lack of a formal framework weakens an organisation's ability to provide consistently strong and timely responses. Stakeholders depending on less formally prepared organisations may suffer from outage durations extending into days or longer.

4. Future network operators may not be recognised as part of the critical infrastructure 🟨 🟩 ⬛🟪

Future network operators may not be recognised as part of the critical infrastructure by Member States or by other industry participants. Conversely, new entrant network operators may not realise that they are part of the critical infrastructure.

Impact: If government and other critical stakeholders do not recognise new entrants as part of the critical infrastructure, the new entrants will not be granted priority treatment in times of crisis. This weakens the robustness of the new entrants' networks, both for their subscribers and for services they may provide for other network providers. Also, without new entrants realising their own critical role, they may not appropriately plan, invest and maintain vital emergency preparedness and disaster recovery capabilities.

5. Government engages network operators too late 🟪

Several industry representatives expressed frustration in that they feel they are often invited to relevant discussions with government too late in the process to have any real input or impact on the outcome.[29] It is disappointing to industry members because they feel their expertise is not being properly utilised. There are also concerns that the industry is being ”involved“ in a superficial way, possibly to give the appearance of being engaged more substantially than they actually are.

Impact: Government does not fully benefit from the expertise which industry possesses and the partnership between industry and government is further weakened.

[29] The original ARECI Study plan was adjusted in recognition of this concern. The original "workshop" that was scheduled for end of the study period and gave the impression of a highly interactive event, was renamed more properly as a "public forum" to more accurately reflect it as an opportunity to receive a read-out of the study's guidance. Four highly interactive experts workshops were held much earlier in the study process (see Methodology, Section 2.3.). The participant feedback for these events was very positive (www.comsoc.org/~cqr/EU-Proceedings-2006.html).

3.2 Basic Level Observations - Maturity Level 2

The 21 observations presented here are representative of an operation that is commonly recognised as part of the communications industry, but is still working on implementing practices and procedures to consistently address routine occurrences in their network. This level may also be reflective of established organisations that are deploying new products or services with which they are not experienced. The stumbling blocks here are not usually technological, but rather procedural.

6. The deployment of priority communication services is awaiting government funding

🟥 🟪

While network operators and service providers are very sympathetic with the need for priority communication services, there is no (or insufficient) business case motivation in the Private Sector to develop, deploy and maintain these services.

Impact: Network operators will not deploy priority treatment of critical calls in public networks until there is government compensation. The absence of such priority treatment means that critical calls will not be given a higher probability of call completion.

7. Multiple standards bodies are producing different standards

⬛ 🟪

Standards are critical, but the way standards are selected varies between organisations and is typically informal. Different service providers and equipment suppliers are using different standards. Usually the differences within these standards are *not* service affecting, however occasionally services do *not* work as expected or fail to work at all. Resolving these problems is difficult as involved parties correctly claim that they are implementing the appropriate standard.

Impact: As different organisations follow similar, but different, standards (e.g., IETF, ITU-T, ETSI, CableLabs) there can be interoperability problems. Such problems may affect: how features work when the functionality crosses multiple networks; if calls/sessions are lost under certain circumstances; administration; traffic counters; maintenance; trouble ticket resolution; and routing patterns. Each of these situations can adversely affect network availability.

8. The provision of power for future networks will be more challenging

🟨 🟩 🟦

Network equipment is becoming more power dense, with a corresponding greater need for cooling.[30] This requires additional planning and engineering to provide for the required thermal capacity and to provide emergency power for the communications equipment and the cooling equipment.[31]

Impact: Future network robustness and resilience will be negatively impacted without power density planning for communications equipment.

[30] A 'Top Concern" from the Proceedings of IEEE CQR, *"Proceedings of European Experts Workshop on Power & Environment,"* Rome Italy, 3 October 2006.

[31] 91% of subject matter experts confirm. Proceedings of IEEE CQR, "Proceedings of European Experts Workshop on Power & Environment," Rome Italy, 3 October 2006.

9. There is a trend for ICT network equipment to be moved outside of central office buildings 🟨 🟩

Moving equipment outside of the central office creates numerous challenges in the areas of power, security and environmental control.[32] For example, providing reliable power to multiple field locations makes the network more susceptible to multiple commercial power outages.

Impact: The architectural shift to distributed networks exposes more network elements to significant risks. Without proper attention to this issue, network outages are likely to increase due to reliance on commercial power at remote sites, security breaches and environmental stresses.

10. Future networks increase subscriber responsibility regarding access equipment 🟨 🟩 🟧

Future networks entail more customer-owned and customer-powered access equipment (e.g., wireless handsets, routers, modems) located outside the controlled central office environment. As a result, subscribers will find it necessary to manage the power needs of their access equipment.[33]

Impact: With equipment that is owned, maintained, and powered by the customer, there is less control of its security, availability, and reliability.

11. High costs associated with security and availability 🟪 🟦 ⬛

Network operators and equipment suppliers are faced with "the same old story" – reliability and security come at a cost and they compete against other spending opportunities, some of which are immediate revenue-generating.

Impact: Future networks will achieve the network reliability levels dictated by market forces. Newer applications will tend to be initially deployed with lower reliability levels.

12. Reliability and security are challenged by the migration to future networks 🟥 🟧 ⬛

The competitive environment places a premium on cost avoidance. As a result, the investments being made in emerging networks may place less priority on system reliability, performance and security.

Impact: The pressure to quickly deploy new features and services may push reliability and security issues to the background. This may make future networks more vulnerable to external (i.e. hacker) or internal (i.e. human error, malicious employee) attacks.

13. Future networks require vigilance in upgrading software 🟪 ⬛

Each of the many promised capabilities and anticipated new services will be achieved through the implementation of new software, and sometimes new

[32] A 'Top Concern" from the Proceedings of IEEE CQR, "Proceedings of European Experts Workshop on Power & Environment," Rome Italy, 3 October 2006.

[33] A 'Top Concern" from the Proceedings of IEEE CQR, *"Proceedings of European Experts Workshop on Power & Environment,"* Rome Italy, 3 October 2006.

hardware.[34] Likewise, small enhancements and corrections will be accomplished through software changes. Observations during this Study suggested that the majority of network operators are inclined to resist or delay immediate software upgrading. Factors may include concerns about the quality[35] of the new software or cost associated with the testing and installation of the upgrade.

Impact: Network operators that do not maintain current software versions could jeopardise network interoperability or could introduce network conflicts with other networks. Either of these situations reduces the availability of the affected networks.

14. Increasing instances of co-location will affect physical security

🟨 🟧 🟩 🟪

New entrants and providers of different applications and services for future networks are co-locating for economic, regulatory or interconnection reasons. The physical security of the co-located equipment can be compromised, either by intentional or accidental interference by people with access to the space, or by malfunctioning equipment causing an environmental problem (e.g., fire, fire suppression).[36]

Impact: Physical security can be compromised by any of the tenants, or their equipment, affecting all equipment at that location.

15. The PSTN/IN signalling network will be exposed to security threats by future networks

🟥 ⬛

The PSTN/IN will continue to be in place while future networks are deployed. The gateways between the PSTN/IN and future networks will expose the PSTN/IN signalling network to threats from future networks.

Impact: The PSTN/IN signalling network will be exposed to increased reliability and security risks unless security measures are applied at the gateways.

16. Greater external threats exist for future networks

🟥 🟩 🟦 ⬛

The communications infrastructure is the infrastructure on which other infrastructures depend and, as such, will increasingly be a target for terrorist activities. The distributed nature of future networks provides greater challenges in protecting diverse physical locations. Further, as voice moves to future networks, it will be exposed to attacks that have been previously seen on computer networks.

Impact: Communications infrastructure will be exposed to increased physical attacks and cyber security attacks.

17. Layered software introduces additional complexity

🟪

Software layering provides discipline in design, but also results in additional complexity and requires coordination among applications and definition of

[34] 2006 European Experts Workshop on Hardware & Software, Proceedings, slide 16, www.comsoc.org/~cqr/EU-Proceedings-2006.

[35] The introduction of new software versions also holds the possibility of introducing new problems and incompatibilities with prior implementations.

[36] 2006 European Experts Workshop on Power & Environment, Issues Voting, slides 9-10, www.comsoc.org/~cqr/EU-Proceedings-2006.

interfaces.[37] Layered software often masks errors in logic in one layer from the layers above, making the detection of the error more difficult.

Impact: Since a layer supports multiple applications, a single error in that layer can be manifested as vulnerabilities in multiple applications.

18. The level of emergency preparedness varies greatly across Europe

🟨🟧 🟩⬛🟪

There is wide variation in the level of preparedness for natural and man-made disasters.[38]

Impact: If a catastrophe occurred, the recovery of critical communications services provided by some European network operators would be unevenly delayed. For similar events, restoration of service might vary between minutes or hours for those organisations most prepared, to days or beyond for organisations less prepared.

19. Emergency information sharing during incidents is limited

🟧🟪

During an emergency incident,[39, 40] information sharing among Private Sector and government stakeholders is ad hoc, informal and largely based on individual, personal relationships.

Impact: Vital information sharing is limited to personal contacts and may exclude many key stakeholder organisations that could benefit from the information. Further, the dependencies on individual personal contacts are single points of failure.

20. Equipment co-location weakens network physical diversity

🟧 🟩🟦⬛🟪

Network operators and providers of applications and services are co-locating for various reasons, and this trend will continue with the deployment of future networks. Physical diversity for both network operators and subscribers can be compromised by co-location sites.

Impact: This concentration of facilities and equipment can result in unintended physical single points of failure that can have a significant impact on overall critical infrastructure. Disasters such as fires or terrorist attacks at such sites could have wide-spread impact.

21. Collaboration between governments and the Private Sector needs improvement

🟪

Collaboration between Member State governments and the Private Sector, as well as between the European Institutions and the Private Sector is viewed as becoming increasingly important. However, this collaboration is currently seen as “poor”. [41, 42]

[37] 2006 European Experts Workshop on Hardware & Software, Proceedings, slide 17, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[38] 2006 European Experts Workshop on Power & Environment, Issues Voting, slides 4-5, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[39] 90% of subject matter experts confirm. Proceedings of the Power and Environment Experts Workshop, Rome, Italy, October 3, 2006. www.comsoc.org/~cqr.

[40] 76% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *“Proceedings of European Experts Workshop on Policy & Human,”* Brussels Belgium, 15 November 2006.

[41] 78% of subject matter experts rated collaboration between the Member State governments and the Private Sector as “poor.” IEEE Communications, Quality and Reliability (CQR), *“Proceedings of European Experts Workshop on Policy & Human,”* Brussels Belgium, 15 November 2006.

[42] 100% of subject matter experts rated collaboration between the European Commission and the Private Sector as “poor.” IEEE Communications, Quality and Reliability (CQR), *“Proceedings of European Experts Workshop on Policy & Human,”* Brussels Belgium, 15 November 2006.

Impact: Governments are missing opportunities to benefit from Private Sector expertise. Lack of collaboration weakens the overall reliability of public networks.

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

Future networks will consist of many components from many suppliers, both in the core network and at the customer premise. These components will have vastly different capabilities, levels of maturity, and sophistication in terms of quality, reliability, and security.

Impact: Combining multiple components and network elements will place an increased burden on network operators to ensure quality, reliability, and security in future networks.

23. Private Sector is disappointed in the yield of government partnerships

Service providers and network operators are aware of the important role of interfacing with government regulators and other government stakeholders, but have difficulty identifying collaborative efforts that they consider as "examples of good partnership." This observation was found to be equally true for incumbents and new entrants. Private Sector opinions were more favourable toward initiatives undertaken with Member State governments than those with European Institutions. Interestingly, for a given government-industry initiative, government entities consistently tended to have more favourable views of the value being generated compared to the views of their Private Sector counterparts.

Impact: Suboptimal collaboration produces suboptimal agreements and policies that in turn impede all parties' abilities to promote network availability and robustness.

24. Government regulators are cautious regarding Private Sector claims

Government regulators have a responsibility to protect the public interest regarding the reliability of communications networks. In carrying out this oversight, government personnel often seek information from service providers and network operators regarding their practices related to network design, network operation and emergency preparedness. However, corporate statements in response to such government queries are often lacking in the frank assessment being sought.

Impact: Government stakeholders may feel compelled to obtain information through legislation if they do not believe they are receiving the information they need voluntarily. This will work against the industry-government partnership that is needed.

25. Companies are not committing appropriate expertise in engagements with government

Government regulators are frustrated that service providers and network operators typically send lawyers and government affairs personnel to government-industry collaborative initiatives dealing with critical infrastructure. They feel that the industry is too often unwilling to commit the direct engagement of its best technical expertise.[43]

[43] Several seasoned government representatives observed that the experts workshops held in support of the ARECI Study contrasted with the characteristic government-industry meeting in large part due to the technical expertise engaged (www.comsoc.org/~cqr/EU-Proceedings-2006.html).

Impact: Government policies suffer from inadequate technical insight and may therefore be less effective in promoting network reliability and security.

26. The Private Sector is not treated by government as an equal partner 🟪

Service providers and network operators do not feel as though they are treated as equal partners when dealing with government entities. This results in awkward dialogue, disengagement of industry expertise, and weakened industry-government collaboration. Government stakeholders did not express a similar feeling about dealing with industry.

Impact: Government policies regarding communication network technology and operations may lack critical insights available from the best experts and therefore fall short of creating the best frameworks for infrastructure availability and robustness.

3.3 Common Level Observations - Maturity Level 3

The 28 observations presented here are representative of a well established operation in the communications industry. This level includes items that incumbent operators usually have addressed but newer entrants may be still working to implement. These findings typically focus on looking outside of one’s organisation and dealing with the issues associated with interfacing with other organisations.

27. Some government leaders are embracing a mindset of preparing for the worst 🟨🟩 🟧⬛🟪

While there is variation regarding the recognition that a catastrophic event can occur in their country, some countries are highly expectant – typically those that had an event (natural or man-made) occur in recent years – and have expended the resources to prepare for responding to future disasters.

Impact: The expectation that a major catastrophe can occur motivates emergency preparedness planning, investment and training. Those governments that are well prepared are role models for others.

28. Priority calling for critical communications in public networks is needed 🟥⬛

Many Member States do not have priority calling[44] schemes that allow critical communications over public networks. Even where separate emergency networks exist, there is often a need to provide called or calling party access to public networks. Public networks are also a backup when the separate emergency network sustains damage or is in overload.[45]

Impact: To the extent that critical calls are attempted on public networks, the probability of call completion is not consistent with the urgency of such calls if they are not provided preferential treatment. The critical stakeholders with not have ubiquitous access or sufficient capacity and resiliency.

[44] Priority calling is defined as a government authorised caller placing a call that is marked as priority by the network and given preferential treatment to increase its probability of completion (also known as authority-to-authority calls).

[45] 2006 European Experts Workshop on Policy & Human, Issues Voting, slides 4-5, www.comsoc.org/~cqr/EU-Proceedings-2006.html

29. Priority restoration for critical subscribers is not commonly supported

Even though society consistently recognises certain users as more critical than others in the aftermath of a disaster, priority service restoration for these subscribers is seldom supported. To accomplish this, network operators need to identify critical subscribers (e.g., public safety responders, hospitals, law enforcement) and associated network facilities in advance, and provide a mechanism to provide priority restoration for these users. Reducing the number of required decisions can help eliminate confusion during incident response. In some cases, national laws prevent such differentiation among subscribers, and so these policies will need to be reviewed.

Impact: Lack of pre-determining which subscribers require priority restoration will unnecessarily delay the restoration to these subscribers.

30. Interconnection testing is not based on a recognised standards-based framework

Many of the incumbent organisations report that their process of testing new entrants for interconnection to their networks is based on their own set of test procedures and observations of the traffic characteristics.[46] Some new entrants may lack experience in the complexities of network interconnections. A mutually agreed standards-based testing framework will bring order and structure to the testing process.

Impact: The informal process will not scale up well as more and more networks seek connection. Lack of a standardised procedure lengthens the interconnecting test period and requires more resources from both the incumbent and the new entrant.

31. Interoperability testing between networks is often an overlooked function

Formal processes for resolving interoperability issues between networks do not generally exist. Many of the organisations depend on informal cooperation at the lowest technical levels to resolve interoperability problems. The intrinsic network vulnerability of “network interconnection” is a major challenge for future networks.[47]

Impact: When the informal approach works, it works well. But when problems fail to get resolved, then it is often more difficult to get them resolved in the absence of a more formalised process.

32. Both incumbents and new entrants consider regulation undesirable

To achieve necessary levels of network reliability, both incumbent network operators and new entrants consider government regulation an unnecessary burden, as market forces dictate acceptable levels of quality and reliability of services, especially in areas where broad competition exists. In addition, government mandates could impede the preferred reliance on expert guidance and are less likely to be effective in keeping up with technology advances.

Impact: Regulations frequently have unintended consequences and may not achieve their desired results.

[46] 50%% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *“Proceedings of European Experts Workshop on Network & Payload,”* London UK, 6 October 2006.

[47] 74% of European network subject matter experts confirmed. Analysis of responses to the Bell Labs ARECI Study Virtual Interview.

33. Time-to-market pressure influences reliability and security

Competitive and business drivers influence decision makers throughout the deployment lifecycle. For example, equipment suppliers must meet delivery schedules and manage competing interests for limited resources, and network operators make trade-offs between delaying roll out of new offerings for independent testing or meeting the market window. While this business reality is not new, this time-to-market pressure, when coupled with the shorter lifecycle of the systems underlying future networks, places greater strain on meeting reliability and security objectives.

Impact: There is increased risk that systems will be deployed and networks implemented with primitive reliability and security functionality and latent design errors, thus undermining infrastructure robustness.

34. Reliability and security metrics for future networks are immature

Future networks will be multi-services networks that support a variety of new applications. Each application will have very specific characteristics (e.g., always on, location and presence services, real-time, store and forward) that will present different stresses to the network. Availability and security metrics need more attention in collaborative efforts.[48]

Impact: The resiliency and robustness of future networks cannot be measured or improved without appropriate reliability and security metrics.

35. Dialogue within industry is limited

Information sharing within the ICT industry is insufficient, especially regarding emergencies.[49, 50] Stakeholders believe that in the past there have been too many forums that proved ineffective. In addition, there seems to be a lack of formal dialogue between network operators of different network technologies and business models.

Impact: Network availability and robustness suffers in the absence of industry dialog leading to inefficient replication of solutions and failure of solutions to interoperate. Establishing dialog can lead to further cooperation and mutual aid.

36. Future networks have a strong dependency on scarce, highly-skilled experts

New technologies require new skill sets, which are not widely available. Many new entrants are quick to enter the market without the number of highly skilled or trained workers needed, and incumbent network operators are deploying new networks that also require these new skills.[51]

Impact: Availability, security and robustness of future networks will be diminished without qualified technicians to maintain them.

[48] 94% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), "Proceedings of European Experts Workshop on Network & Payload," London UK, 6 October 2006.

[49] 73% of subject matter experts confirm. Proceedings of the IEEE CQR Power and Environment Experts Workshop, Rome, Italy, October 3, 2006. www.comsoc.org/~cqr.

[50] 76% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Policy & Human,"* Brussels Belgium, 15 November 2006.

[51] 69% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Hardware & Software,"* Berlin, Germany, 11 October 2006.

37. Feature interoperability between legacy networks and new networks is complex

Feature interoperability can be provided by either feature emulation or simulation. Simulation provides an exact feature match, while emulation provides the same service but with possible observable differences in operation. Testing of these interactions is a complex process, especially across multiple networks.

Impact: Failure to address these issues can result in lost sessions or sessions where the feature experience is not what the customer expected, resulting in customer dissatisfaction.

38. Equipment co-location breeds environment and operational concerns

Network operators and providers of applications and services are co-locating for various reasons, and this trend will accelerate with the deployment of future networks.[52] Environment conditioning and operational coordination with co-located operators requires additional planning and consideration, as individual service providers have less direct control of these issues.[53] Competition for shared space, common connection points, power (both commercial and emergency) and access control between tenants of shared space must be governed by prior agreements, especially in cases of disaster recovery.

Impact: Coordination at co-location sites is vital to the resiliency of public networks.

39. Future networks will be more difficult to manage

Coordination between different networks architectures with equipment from multiple suppliers and a large number of highly interfaced systems presents new challenges for managing future networks. Network maintenance and vendor support procedures will need to accommodate these challenges.

Impact: Coordination between network operators and vendors' support becomes increasingly difficult in future networks, and may extend some outage durations.

40. Agreements, Standards, Policies and Regulations (ASPR) are Member State dependent

Individual stakeholder networks and services are likely to cross Member State borders and are therefore subject to differing agreements, standards, policies and rules. Different ASPRs may require network operators to deploy multiple configurations and software concurrently in a single node when it spans multiple Member States.

Impact: Different ASPRs complicate network design, interconnection and recovery issues.

[52] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 9, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[53] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 10, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

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

Many local governments[54] are providing access to government services and databases, and network access to the public, but do not have a "security culture".[55] It may not be evident to government administrators that this network access and these government services are part of the critical infrastructure and have a direct impact on other network infrastructures.

Impact: The reliability and security of local government networks directly impacts the networks to which they connect, and must be treated as critical infrastructure.

42. The rigor of reliability and security programs varies widely across network operators and service providers

The levels of rigor in supporting network reliability and security differ among network operators due to variations in awareness of best practices, degrees of experience and understanding of their role as critical infrastructure provider. The Study has shown that new entrants tend to have simpler reliability and security programs.

Impact: The result of different levels of program rigor will be a reduction of the level of reliability and security to that of the weakest element.

43. Security approaches used by the PSTN/IN are not sufficient for future networks

Future networks are more sophisticated than today's PSTN/IN network. They include more layers, are more complex, contain more multi-vendor equipment and software, and are more distributed, both physically and functionally. Security mechanisms for future networks will need enhancements over those used on today's PSTN/IN network.[56]

Impact: Many more security vulnerabilities of different characteristics and at different locations exist in future networks. PSTN/IN security approaches, while useful, will not fully address all of the security vulnerabilities associated with future networks.

44. Future networks create signalling traffic security and reliability challenges

PSTN/IN signalling has been relatively secure because the signalling traffic is segregated onto separate physical links (e.g., C7) and the interconnections are made between large service provider "trusted" networks. This trusted environment cannot be ensured in future networks due to signalling across networks implementing various levels of security.

Impact: Lower levels of security in some networks can act as an entry point for attacks into more secure networks. Signalling is more vulnerable to corruption and other security attacks (e.g., DDoS).

[54] This may be equally applicable to private enterprises.

[55] 2006 European Experts Workshop on Power & Environment, Proceedings, slide 12, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[56] Proceedings of the IEEE CQR Workshop on The Trust Paradigm, Washington, D.C., October 17, 2006. 80% of security experts disagreed that "the security needed for ICT can be achieved by existing approaches". 80% of security experts consider the Common Criteria approach to be "seriously falling short" and 100% consider it to be too slow. (www.comsoc.org/~cqr).

45. Distributed nature of future network functions may impact availability

Applications and future network functions rely heavily on a distributed functional architecture and functions may be implemented across physical network elements. Software may run on individual cards, across multiple cards within a network element, or across network elements.

Impact: There are more physical entities and associated software where failure or attack may occur, resulting in a network, an application, or a service becoming unavailable.

46. Increased number of less mature future network elements may impact availability

Future networks will be composed of many network elements which do not have the reliability maturity of the PSTN/IN. Since operational experience for these entities is in its infancy, their impact on network availability is unknown.

Impact: Unless careful engineering of future networks and routine updates to the operational methods and procedures are performed, network availability may suffer due to the disparate reliability of the various network elements.

47. Current PSTN/IN applications may be limited initially on future networks

Future networks may not offer all of the same features that are currently provided on the PSTN/IN (e.g., central office based speed dial is a feature that will not likely be replicated), and some customer premise equipment will not be compatible with future networks. Therefore, provisions will need to be made for subscribers to adapt to the change.[57] In addition, future networks will support new features, requiring interoperability between the PSTN/IN and future network features.

Impact: The migration to future networks will not be transparent and the risk of feature or functionality loss is increased.

48. Future networks may not support PSTN/IN data services

Data service emulation/simulation of some PSTN/IN services has not been fully defined for future networks, nor has the inter-working of data services been defined.

Impact: Until these capabilities are provided, and their reliability and security have been proven, end-users will be concerned with the loss of data services.

49. Future networks contain application elements whose failure can cause major outages

All network subscriber, service, and application data for a particular network may be located in a small number of functional entities (e.g., Home Location Register (HLR), Home Subscriber Server (HSS), applications servers, related data bases). These functional entities may be implemented on one or more network elements that may not be in a controlled environment.[58]

[57] Standards are being developed for service emulation (i.e. same functionality and operation) and service simulation (i.e. equivalent functionality, operation may differ).

[58] 2006 European Experts Workshop on Power & Environment, Proceedings, slide 18, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

Impact: A site disaster, interoperability problems, or even a power failure can have severe availability impacts (e.g., time to restore) since the functional entities contain subscriber data and network state information for a very large population. Service via other networks will also be impacted.

50. Future networks contain signalling elements whose failure can cause major outages

Critical signalling elements (e.g., Call Session Control Functions) may serve very large populations and cover extended geographical areas. The reliability of the signalling elements and reliability characteristics (e.g., active/standby, switchover) are unknown and/or unproven.

Impact: Although critical signalling elements are typically built on highly reliable redundant platforms, a failure and/or a site disaster can cause loss of service to millions of subscribers and will impact service via other networks. In case that node goes down, there may not be a mechanism for the subscriber to be served by another critical signalling element.

51. Net Neutrality may be misunderstood

Net Neutrality provides a flat transport network where one service provider's packets are not favoured over another's packets in the core network. However, while service providers are treated equally, different applications (e.g., e-mail, voice, video) have different classes of service and thus different priorities. Packets associated with emergency communications also receive priority treatment.

Impact: Misunderstandings regarding Net Neutrality may cause confusion, and customer and service provider dissatisfaction.

52. European communications industry experts confirmed core set of Best Practices

Service providers', network operators' and equipment suppliers' experts have confirmed a core set of Best Practices as effective in promoting network reliability and security.[59] These Best Practices deal with each of the eight ingredients of communications infrastructure.[60]

Impact: Network reliability and security will be optimised by continued industry collaboration.

53. Private sector implementation level of European-confirmed Best Practices is high

Service providers, network operators and equipment suppliers are implementing European-confirmed Best Practices to a high degree.[61] Incumbents in the market place tended to have higher implementation levels compared to new entrants.

[59] 100% of subject matter rate the Best Practices as highly or moderately effective from: the IEEE Communications, Quality and Reliability (CQR), "Proceedings of European Experts Workshop on Network & Payload," London UK, 6 October 2006; IEEE Communications, Quality and Reliability (CQR), "Proceedings of European Experts Workshop on Hardware & Software," Berlin, Germany, 11 October 2006; IEEE Communications, Quality and Reliability (CQR), "Proceedings of European Experts Workshop on Policy & Human," Brussels Belgium, 15 November 2006.

[60] Power, Environment, Hardware, Software, Network, Payload, Human, Policy/ASPR (see Eight Ingredient Framework, Section 2.2.1).

[61] Best Practice Effectiveness Survey, Section 2.5.3.

Impact: Network availability and robustness are optimised when industry experts have access to industry consensus guidance and are free to make local decisions regarding appropriate implementation.

54. There are too many studies, initiatives, reports and recommendations
Industry and government stakeholders are involved in an ever-increasing number of activities dealing with the broad subject of infrastructure reliability and security. The pressure to support these many activities stresses the limited available staff, at times beyond their ability to be effectively engaged. The large number of activities produces many reports and many recommendations which also must be reviewed and acted upon, further straining the available staff. Some stakeholders suggested that the reason there are so many activities is that so few are effective and many re-attempts emerge in reaction to the limited progress of previous efforts.

Impact: Limited government and industry resources are drawn in many different directions and therefore the pace of achieving consensus is slower than necessary.

3.4 Advanced Level Observations - Maturity Level 4

The 29 observations presented here are representative of an operation that has begun implementing new strategies to deal with the nuances associated with interfacing future networks with legacy networks. This level includes items to address the realities of changing threats to critical infrastructure and working cooperatively with other organisations in the industry.

55. Authorisation of priority communications users must be managed
A means of caller authorisation is required for government-authorised priority calls using public networks. Examples of these users are emergency first responders, law enforcement personnel and national security officials. In future networks, this will include both voice and other applications such as data and video.

Impact: Validation of a user attempting to make a priority call allows the network to determine whether priority treatment is warranted. The absence of this validation creates a vulnerability for a Denial of Service (DoS[62]) attack.

56. IP-based emergency communications services have not been deployed
Worldwide industry standards bodies, addressing both national and international operations, have developed initial standards for emergency communications services for IP networks[63] but these capabilities have not been generally deployed by network operators.

Impact: Until deployed, priority communications services will not be available on IP-based networks. Critical priority communications will not complete with a high degree of probability during periods of high congestion.

[62] A malicious attempt to render a computer resource unavailable to its intended users.
[63] The following standards bodies are continuing their work to enhance these standards: IETF IEPREP, ITU-T SG 2 and ITU-T SG 11 for international, ETSI TISPAN and ATIS PTSC for national.

57. Future networks have the opportunity to introduce mechanisms for early warning services 🟥⬛

Early Warning[64] calls are generally not supported. It should be noted that cable networks do provide Early Warning to their subscribers as part of their basic service (i.e. television), and could provide Early Warning for other applications (e.g., VoIP, Internet) over their existing infrastructure.

Impact: Future networks provide Member States with the opportunity to develop and deploy new Early Warning capabilities to enhance public notification during disasters. When this capability is deployed, future networks must be prepared to handle the level of traffic (i.e. mass calling blast) that it will generate.

58. Mutual aid agreements are essential for effective incident response 🟨🟧🟦⬛🟪

Coordination between many companies, as it relates to incident or disaster response, is informal, especially with new entrants. With an informal approach to emergency preparedness, mutual aid agreements lag even further behind in terms of structure and procedure.

Impact: During response to disasters, companies will be preoccupied with their own recovery operations. Without pre-established mutual aid agreements, the likelihood of a coordinated industry response to an emergency situation is greatly diminished. This takes on added significance when multiple service providers are located in a common facility.

59. Critical communications infrastructures lack priority restoration agreements 🟨🟩⬛🟪

Formal agreements with other infrastructures (e.g., electrical power) to provide priority restoration to communication facilities generally do not exist.[65] Such agreements are can greatly enhance the robustness of critical communications services following a disaster.

Impact: Delay in obtaining restoration from supporting infrastructures (e.g., electrical services) can have a significant negative impact on providing uninterrupted critical communications services.

60. Emergency exercises are essential in preparing for disasters,[66] but are not being sufficiently utilised 🟨🟩🟧⬛🟪

Periodic testing of emergency plans is not a common practice for most network operators.[67] Most service providers believe they have some type of plan, but for some companies, this only exists as a general mental picture and is not routinely practiced.

[64] Early warning calls (also known as Authority-to-Public calls) provide the ability for an authorised agency to place a warning call to all subscribers in a geographic area.

[65] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 11, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[66] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 6, www.comsoc.org/~cqr/EU-Proceedings-2006.html, and 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 2, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[67] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 7, www.comsoc.org/~cqr/EU-Proceedings-2006.html, and 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 3, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

Impact: Emergency response plans must be flexible enough to adjust to specific situations, however the only way to verify the framework of a plan is to periodically exercise it. Exercises also provide the people who participate in them with valuable experience that enables them to provide a much quicker and more efficient response to emergency incidents.

61. Security integration and interoperability testing guidelines are inconsistent

🟪🟥🟧⬛🟪

Some network operators have direct oversight on testing, utilizing a strong lab environment, while others rely on supplier testing that cannot encompass all possible implementation environments (i.e. interfaces with other systems). The issue exists for integration within individual networks, between two or more technologies and between two or more networks.

Impact: There will be difficulty and ultimately greater expense in ensuring that end-to-end services and their security functions will work as desired.

62. Network operators interface without joint Quality-of-Service (QoS) and performance agreements

⬛🟪

Network performance objectives are typically set internally as “best effort”. Because such efforts yield variable results, many end-to-end performance objectives are not yet defined nor addressed.

Impact: The absence of a uniform set of goals results in non-uniform customer end-to-end QoS experience.

63. Call admission control is not being widely used as a means of overload control

🟪🟥⬛🟪

Many operators do not have a set of requirements for Call Admission Control (CAC[68]). Current approaches for dealing with high network traffic conditions rely on over-engineering capacity so that all offered payload can be handled without degradation. In the near future (i.e. 2010), the offered payload will dramatically increase, thus significantly reducing excess network capacity. CAC, typically defined in Service Level Agreements (SLA’s), will mitigate this bandwidth demand and become essential as traffic levels grow.[69]

Impact: Without Call Admission Control, future services will experience frequent and sometimes severe degradation due to traffic overloads.

64. Many network operators do not prioritise packets

🟥⬛🟪

Packet prioritisation both within and between networks is essential for healthy network maintenance and administration. In order for a network to gracefully recover from an outage, it is necessary that the control messages be given priority treatment between the nodes that compromise the network to ensure they are not dropped or delayed. Many of the operators do not have a scheme for prioritisation of packets, especially between networks.

[68] CAC is further discussed in Annex E.

[69] 100% of subject matter experts confirm that CAC is essential in future networks. IEEE Communications, Quality and Reliability (CQR), *“Proceedings of European Experts Workshop on Network & Payload,”* London UK, 6 October 2006.

Impact: The absence of packet prioritisation will degrade the ability to perform network management and recovery during high traffic levels.

65. Future networks will rely on dynamic network controls

Manual response to network events is becoming less viable. The speeds of transmissions and signalling traffic, the rapidity and intensity of incidents (e.g., attacks) and the frequency of attacks will increase. Automatic network monitoring and actions controlled by artificial intelligence provide the capability to handle these rapid changes.

Impact: Because significant control is being shifted from human decision-making to automated processes, society will be routinely entrusting artificial intelligence to ensure the reliability of its communications. Hardware and software design or implementation errors in support systems can have a far reaching impact on communications services.

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

Outsourcing of hardware and software development presents several problems.[70] These include general lowered levels of control, reduced access to the developers and exposure to programmer loyalties.[71] In addition, timeframes for program fixes are less predictable.[72]

Impact: Outage recovery may be impacted by inefficient access to development teams. Programmers with divided loyalties have opportunities to undermine system integrity.

67. Future networks provide wider access to network controls

The interconnectedness of the network elements in future networks greatly increases the number of sources of network control messages. Some of these interfaces will allow the exchange of network control messages per defined protocols. Such architecture and protocols extend greater control capabilities for external operations staff and even subscribers.[73, 74, 75]

Impact: Future network architectures are more susceptible to insider and subscriber attacks.

[70] 86% of subject matter experts believe the risk is significant. Proceedings of the IEEE CQR Hardware and Software Experts Workshop, Berlin, Germany October 11, 2006. www.comsoc.org/~cqr.

[71] 2006 European Experts Workshop on Hardware & Software, Issues Voting, slides 18-19, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[72] 86% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Hardware & Software,"* Berlin, Germany, 11 October 2006.

[73] For example, in 3G networks, both the user plane as well as control plane use Session Initiated Protocol (SIP) signalling and hackers can take advantage of this situation to impair networks.

[74] 73% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Network & Payload,"* London UK, 6 October 2006.

[75] 77% of subject matter experts confirm that open source software negatively impacts reliability and security. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Hardware & Software,"* Berlin, Germany, 11 October 2006.

68. Established sessions will traverse diverse network technologies as they follow mobile users

Future networks will offer many new services with the expectation that they can be supported for mobile applications. This support includes being able to continue an existing session[76] as one moves among, and accesses, different networks. As these networks can deploy different technologies,[77] the hand-offs for these active sessions require nontrivial coordination.[78]

Impact: Without cross-network session coordination, mobile users will encounter dropped calls or sessions, and thus experience degraded service reliability.

69. Local governments play a key role in educating the public and providing funding for network security

Local governments can further the education of the public on the need to include security in the public's use of network services.[79] This can be accomplished by requiring security measures for interaction with government services, providing public security awareness training, and funding security initiatives.[80]

Impact: Network access to government services may be one of the first services that new user's access. Making security an integral part of the experience will reinforce the importance of security in all electronic communications services.

70. Information sharing of network security incidents with Member States is limited

Some Member States do not routinely receive security incident reports, although security incident response and reporting is done informally among some network operators. There are national and cultural sensitivities concerning any centralised security incident reporting to a government entity. In addition, some Member States have not established an authorised agency to receive and process such reports. Such information sharing is essential in early recognition of the nature and extent of an incident.

Impact: Information sharing can provide government stakeholders with early warnings regarding network problems and engage the support of governments early should their support be needed.

71. Security standards are inconsistently implemented

Stakeholder's participation in security standards development and awareness of current standards varies substantially. This wide range in participation contributes to inconsistent implementation of security standards, deficiencies in interoperability testing of security mechanisms, and weakness in the overall security of connected networks.[81]

[76] a session includes a voice call, video or other application.

[77] e.g., WiFi, WiMAX, and 3G.

[78] Voice Call Continuity (VCC) allows the transference of an active call session from one technology to another (e.g., a call can be switched from cellular to WIFI as the subscriber enters a different environment). These networks will have disaggregated and geographically distributed network functions that encompass multiple databases, application servers or gateways.

[79] 2006 European Experts Workshop on Power & Environment, Proceedings, slide 15, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[80] 85% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Hardware & Software,"* Berlin, Germany, 11 October 2006.

[81] 64% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Hardware & Software,"* Berlin, Germany, 11 October 2006.

Impact: Increased security risks exist when organisations do not deploy equipment based on the most current security standards. Increased security risks in one network adversely affect the security of all networks.

72. Protecting networks from misuse requires comprehensive security design 🟪🟥

Network misuse (e.g., identity theft, session hijacking, rogue certificate authority) affects network users but may not impact network operation. Network attacks (e.g., network time bombs, DDoS) may render the network unavailable to authorised users. Both types of attacks have serious implications on network reliability and user expectation and must be addressed.[82, 83, 84]

Impact: Security designs not based on a comprehensive understanding of network security threats and vulnerabilities will result in weakened network security and availability.

73. End-users' awareness of security issues and end-user device security setting is lacking 🟧

Network operators and service providers believe that end-users need to be educated particularly about VoIP and WiFi security risks and end-user device security settings. Several stakeholders already have public awareness campaigns in progress. Of course networks still need to have protection built in rather than rely solely on end device security.[85]

Impact: Absence of security knowledge results in higher security risks for both end-users and the networks. End-user device security that is not turned on by the user offers no protection.

74. Federated Identity Management will become a compelling security strategy in future networks 🟥🟪

Future networks will not be able to assure the identity and certificates for all applications and services with a single authority due to the number of services and the complexity of applications and services. A Federated Identity Management system,[86] will be needed to allow for identity management across network security domains.[87]

Impact: A Federated Identity Management system mitigates these concerns and provides users with a more efficient and more secure interface.

[82] Stakeholders need to be aware of the ITU-T X.805 and ISO/IEC 18028-2 framework for addressing these network security issues in a systematic and comprehensive fashion. See Annex C for a detailed description of this framework.
[83] 69% of subject matter experts confirm the need for development guidelines. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Hardware & Software,"* Berlin, Germany, 11 October 2006.
[84] 67% of subject matter experts confirm the need for consistent security metrics. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Hardware & Software,"* Berlin, Germany, 11 October 2006.
[85] 93% of subject matter experts agree that greater end-user security and reliability is required. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Hardware & Software,"* Berlin, Germany, 11 October 2006.
[86] Federated Identity Management is a system that allows individuals to use the same user name, password, or other personal identification to sign on to multiple networks.
[87] 64% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Hardware & Software,"* Berlin, Germany, 11 October 2006.

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

Malicious use of end-user devices can generate more intense traffic and access internal network functions. The ability of end-users to send signalling and management messages creates new vulnerabilities for future networks (e.g., SIP traffic from unauthorised sources).[88]

Impact: This vulnerability allows a malicious user to create a network overload that could result in failed calls for subscribers, including emergency calls. The malicious user may also modify or bring down the network by gaining access to signalling messages.

76. Third party components may have an adverse impact on networks

The use of third party components makes it difficult for equipment manufacturers to determine what security standards have been followed, and the level of security enforced throughout the supply chain. Components may contain built-in defects, either intentional or unintentional, and it is more difficult to identify, control, and repair these defects when a third party supplier is involved.[89]

Impact: Detecting and resolving problems will typically take much longer when components from third parties are flawed.

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

Service providers will have an increasingly difficult time verifying the integrity of the supply chain for future networks, which is composed of distributed components from multiple vendors. The introduction of equipment from multiple new vendors increases the risk of unknown vulnerabilities being introduced into the supply chain, and places the burden of trouble isolation and resolution between multiple vendors on the primary service provider.[90, 91]

Impact: New vendors are a potential vulnerability in the supply chain until they have established themselves and their security processes. Service providers will need to be vigilant as they integrate equipment from new vendors into their network.

78. Scaling problems in future networks are expected

Initially, future networks will be lightly loaded and experience with database, server, and security feature scaling and bottleneck identification will be limited. Service providers and equipment suppliers may not understand new equipment scalability factors and limitations for wide-spread growth.

Impact: The inability to handle increased and focused traffic as the network grows may compromise performance.

[88] 2006 European Experts Workshop on Network & Payload, Proceedings, slide 25, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[89] 94% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Policy & Human,"* Brussels Belgium, 15 November 2006.

[90] 94% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Policy & Human,"* Brussels Belgium, 15 November 2006.

[91] 86% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Hardware & Software,"* Berlin, Germany, 11 October 2006.

79. Introduction of network security may impact service availability

Future networks require enhanced network security (e.g., network intrusion detection and protection systems) but cannot be done without considering the impact upon the underlying applications. Adding network security may affect service availability by introducing choke points and other potential points of failure.

Impact: Network performance, capacity, and availability may be impacted by security measures and must be considered during network engineering.

80. Cascading failures of a hardware component or a software element require new management strategies

A single hardware component or software module that is widely deployed magnifies a vulnerability caused by an inherent defect in that component or element. Multiple vendors using the same hardware component or software module in various applications may compound the vulnerability. Thus, the network is more susceptible to catastrophic failure due to widespread failures of a single component type in a short period of time.[92]

Impact: A widely deployed single component or module with a high failure rate in diverse equipment will have profound impact on network reliability.

81. Multimedia traffic on future networks will fundamentally change how networks are managed

Video and multimedia traffic on future networks will dramatically increase the bandwidth requirements. It is essential to study and model the likely traffic patterns to better understand the impacts on network capacity. By understanding the traffic patterns, management processes and procedures can be developed.[93]

Impact: Network providers will not be able to react quickly enough in real-time to rapidly changing bandwidth demands. Multimedia modelling allows the network providers to deploy equipment before the demand exceeds capacity.

82. Sessions traversing diverse networks result in various degrees of QoS

As sessions transverses diverse networks with different technologies, the end-to-end QoS of that session is a function of the service provided by each network and the transition gateways. This represents a balance between end-to-end QoS and the subscriber's desire to use diverse access technologies.

Impact: Transitions across network boundaries could adversely affect the end-to-end QoS of the session, making it more difficult to provide expected service quality and performance.

[92] 2006 European Experts Workshop on Hardware & Software, Proceedings, slide 20, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[93] Listed as a top concern in the Proceedings, IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Network & Payload,"* London UK, 6 October 2006.

83. Opportunity to incorporate accommodations for people with handicaps
As future networks are developed, there is a unique opportunity to incorporate accommodations[94] that will provide equivalent service experience for people with handicaps. Such accommodations have historically been considered only after the basic services were defined and deployed. These were then added to the architecture as exceptions rather than being seamlessly integrated. One example is the Telephone TeletYpe (TTY) service for people who are deaf, hard of hearing, or speech impaired.

Impact: By incorporating these accommodations in the initial architecture, people with handicaps will be more fully included in benefits of future networks and additional costs and inefficiencies will be avoided.

3.5 State-of-the-Art Level Observations - Maturity Level 5

The 17 observations presented here are representative of an operation that has embraced the challenges of future networks and is leading the way in addressing those challenges. The technologies associated with this level may still be in their infancy or may not have been invented yet. This category includes developing and implementing policies for which there may be no current standard and looking beyond themselves to the industry as a whole.

84. Disaster recovery arrangements across national boundaries are limited
Pre-arranged disaster recovery planning, exercises and assessments across national boundaries are not high priorities for most network operators and Member States. During disasters, mutual aid is too often on an ad hoc basis without coordination across national boundaries.

Impact: The lack of pre-arranged disaster recovery agreements will delay network and service recovery and will have adverse impact on the EU economy.

85. Several Member States have separate communications networks for critical functions
Having separate emergency communications networks allows authorised users to operate among themselves without interference or congestion from the public. While the separation of the networks is logical, the degree of physical separation is not assured.

Impact: Private networks provide capacity and QoS during times of emergency, which is unaffected by congestion on the public network.

86. Priority communications mechanisms are needed between Member States
There is currently no consistent mechanism for extending the priority call treatment between Member States.[95]

[94] Towards an inclusive future (Impact and wider potential of information and communication technologies), Edited by Patrick R.W. Roe EUR: 22562 ISBN: 92-898-0027, © COST 219ter, 2007. Published by COST, Brussels. COST is supported by the EU RTD Framework Programme.
[95] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 5, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

Impact: Critical communications during an emergency between critical stakeholders across Member State boundaries will have a lower probability of completion than is warranted, impairing vital communications during a pan-European event or incident. Human life can be negatively impacted and lack of coordination will slow down the disaster recovery efforts.

87. Validation of user authorisation to place priority emergency calls does not address inter-network calls 🟥⬛🟪

Member States have not established national policies and international agreements to address the validation of these calls as they pass through multiple networks. Standards work is underway to provide procedures and protocol to support international emergency calls.

Impact: Without these policies, critical calls between Member States may fail when they do not receive authorisation and hence preference in a highly congested network

88. Member States do not have a unified influence on communications standards 🟪

Multiple industry organisations and network operators may be participating in standard bodies as representatives of their Member State, but individually do not influence standards as forcefully as they could with a unified European voice.[96]

Impact: Member States have a weaker influence at the standards bodies because they have not coordinated their efforts nor focused on commonality.

89. Collaboration between stakeholders in the United States is perceived to be more mature than in Europe 🟪

The collaboration among United States service providers, network operators and equipment suppliers is considered by European stakeholders to be more advanced than that taking place in Europe. There is specific awareness of activities of industry-government-academia such as the ATIS Network Reliability Steering Committee (NRSC) and the Network Reliability and Interoperability Council (NRIC).[97]

Impact: Consideration of the United States industry cooperation model may yield insights for leveraging European expertise.

90. United States industry experience in dealing with disasters yields valuable learning experiences 🟨🟩 🟧🟪

European industry stakeholders view the United States communications industry as having valuable emergency preparedness and disaster recovery experience.[98] In addition to the participation of several network operators simultaneously in most markets, the United States has learned from several recent crises that spanned

[96] 88% of subject matter experts agree that a coordinated European standards positions would be valuable. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Policy & Human,"* Brussels Belgium, 15 November 2006.

[97] 100% of participants in the Bell Labs ARECI Study Tier 1 interviews recognised the U.S. as a generally strong role model for communications network reliability and security. Much of this is credited to the industry cooperation that exists.

[98] 100% of participants in the Bell Labs ARECI Study Tier 1 interviews recognised the U.S. as a generally positive role model for disaster recovery.

terrorist attacks, infrastructure collapse (power blackout), and natural disasters in the form of hurricanes and floods.

Impact: Consideration of documented lessons learned can aid in European emergency preparedness and disaster recovery.

91. Minimal network management information is shared between backbone network operators and access service providers

🟥 ⬛ 🟪

Access service providers cannot adequately control the call admission rate without knowledge of traffic levels in the backbone network, nor can backbone operators dynamically configure their network without knowledge of the potential offered load. A standard means of sharing this information would help each network maintain the QoS of sessions by allowing effective end-to-end call admission control.[99]

Impact: Without this visibility, end-to-end quality of service will be impaired when there is congestion in the backbone.

92. There is minimal information sharing between critical sectors

🟧 🟪

Network operators are aware of this gap and the need for inter-sector communication, especially during disaster recovery. The general impression of the network operators was that they would benefit from meaningful interaction with other critical sectors.[100]

Impact: Because of significant critical sector interdependencies, problems with communications networks will adversely affect the other critical sectors, and problems within other critical sectors will adversely affect the communications sector. The current communications paradigm contributes to undesirable delays in service restoration.

93. Future networks need to discover end-user device capabilities

🟥 ⬛

Future networks need to have the ability to discover the capabilities, capacities, and characteristics of end-user devices to efficiently manage the network resources that are offered to that end-user device.[101] Inefficiencies are introduced if resources are dedicated to end-user devices that aren't capable of using them or will not be using them for a particular session. Also, there may be additional security aspects that the network must consider with highly capable end-user devices.

Impact: Failure to do real-time network monitoring and management will result in congestion or wasted resources and may expose the network to additional security threats.

94. Future networks must accommodate end-user device feature profiles

🟥 ⬛

The increased capabilities of end-user devices will encourage differential operation and feature offerings based on the unique characteristics of the end-user device.

[99] IETF Pre-Congestion Notification Working Group (PCN) is developing a standard.
[100] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 16, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[101] 2006 European Experts Workshop on Network & Payload, Proceedings, slides 24.25, 27, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

Future networks will be more flexible to accommodate a wide variety of devices and capabilities, creating custom services.[102]

Impact: Without advanced capabilities of networks to discover end-user device profiles, subscribers' services may be unavailable.

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

Legacy network architectures provided separation between critical network control signals and subscriber traffic.[103] Future network architectures co-mingle these two types of information as they traverse the network. This presents both reliability and security challenges for network operators.[104] For example, a malicious subscriber or software design error could insert harmful network control messages.

Impact: The lack of network control message isolation is a fundamental risk to the integrity of future networks. The exploitation of this weakness could result in widespread network outages.

96. End-to-end security is implemented hop-by-hop

Although security[105] is needed end-to-end, it is implemented hop-by-hop or within a network domain. Typical sessions will involve multiple operators and as security is accomplished on a link-by-link basis there is an absence of an overall end-to-end security confirmation.

Impact: Hop-by-hop security may give the impression of overall security but is inherently less secure than end-to-end as there is an absence of overall security criteria.

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

Different businesses have different approaches to achieving reliability and security for their networks. This variation is due to different network architectures, different regional contexts, and different business models and approaches. Industry can benefit greatly from collaboration with the aim of capturing its collective insights and agreeing on Best Practices.

Impact: Consensus European Best Practices will be stronger than the practices that any one organisation can develop on its own. The availability and robustness of public networks will therefore be enhanced by such a collaborative undertaking.

98. Europe has positive information sharing role models

Effective information sharing is very beneficial but difficult to achieve. This is due to the sensitivity of the information involved, the trust needed among participants and the long term commitment necessary by organisational leaders and experts. Europe

[102] 2006 European Experts Workshop on Network & Payload, Proceedings, slide 24, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[103] This is accomplished by Signalling System 7 (SS7) out-of-band signalling.

[104] 73% of subject matter experts confirm. IEEE Communications, Quality and Reliability (CQR), *"Proceedings of European Experts Workshop on Network & Payload,"* London UK, 6 October 2006.

[105] For example, IPSec, end-user identification and authentication.

hosts best-in-class information sharing programs.[106] The attributes of existing programs include high levels of trust, meaningful information sharing and appropriate structuring around interests.

Impact: The benefits of effective information sharing include early awareness of critical concerns, enhanced knowledge and improved ability to defend against attacks.

99. Intelligent handsets can propagate network security incidents

Intelligent handsets are programmable and therefore susceptible to viruses and other malicious software (e.g., Trojan horses).[107] These viruses may then be spread through the network to other end-user devices, or to the network itself.

Impact: Intelligent handsets must be considered an integral part of the network. By extending the network to these devices, the vulnerabilities of these devices must be addressed by the network security plan.

100. Future networks will require automated 'security status' monitoring capabilities

Detecting security violations quicker allows the network to recover more rapidly and protect itself from ongoing attacks.[108] The speeds with which these attacks can propagate render manual action too slow to react and protect, so this automated capability needs to be built into the network.

Impact: Future networks may not be able to survive a security attack if they only rely on manual detection and action.

[106] Warning, Advice and Reporting Points (WARPs) and National Infrastructure Security Coordination Centre (NSCC).

[107] 2006 European Experts Workshop on Network & Payload, Proceedings, slide 25, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[108] 2006 European Experts Workshop on Network & Payload, Proceedings, slide 23, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

3.6 Statistical Summary of Key Findings

The 100 Key Findings were mostly frequently associated with the network ingredient (65), followed by ASPR (57) and then payload (43). Figure 9 provides a Pareto chart depicting the frequency for which each of the eight ingredients was associated. Given the emphasis of this Study on future networks, and challenges working in the European political environments, the top three ingredients being network, ASPR and payload is not surprising.

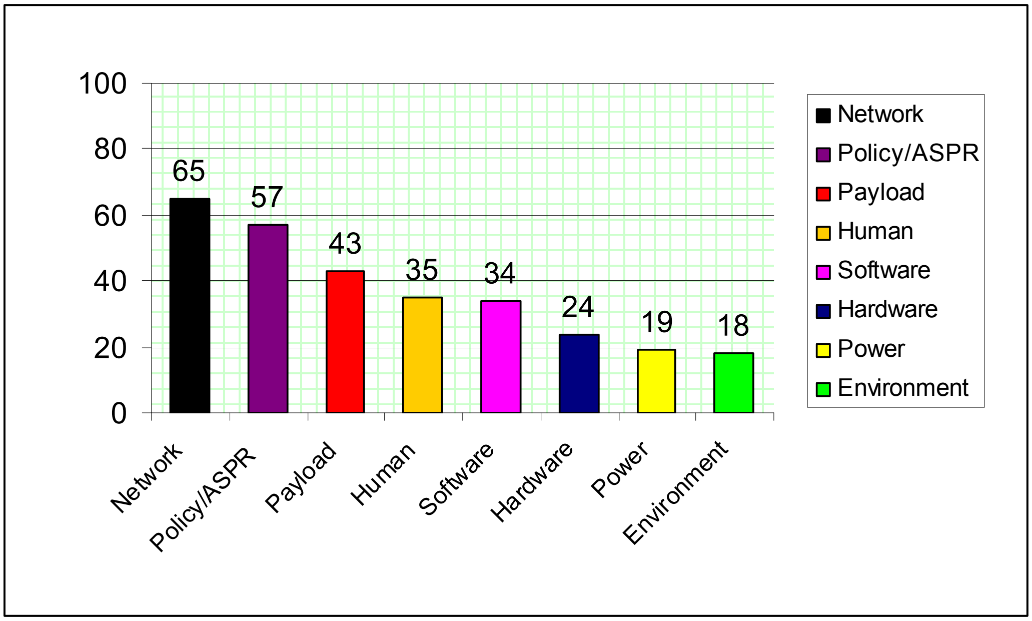


Figure 12: Summary of Key Finding Association with Eight Ingredients

4 RECOMMENDATIONS

The Study's major guidance is presented in this section in the form of ten Recommendations. These Recommendations, if implemented, will significantly enhance the availability and robustness of Europe's communications networks. These Recommendations were developed based upon European stakeholder perspectives, technical policy development experience, the insights captured in 100 Key Findings and expertise in the areas of network reliability, network security and emerging technologies. Each Recommendation was reviewed and supported by stakeholders.[109]

Posture of Private Sector and European Institution and Member State Governments

Each Recommendation requires the active support of the Private Sector and government – both European and Member State. Table 4 provides an overview of the primary leadership role(s) for each Recommendation. Given the requirement of keeping nation-state security interests in the control of Member State sovereignty, an important observation here is that primary leadership roles are largely left to the Private Sector and Member States. This is important because the availability and robustness of public communications networks is inseparably tied to *both* the European Institution-scope social and economic interests and the Member State-scope interest of nation-state security.

Table 3: Summary of Required Leadership Posture

Recommendation	Private Sector	Member States	European Institutions
1	L	AS	AS
2	AS	L	AS
3	L	AS	AS
4	AS	L	
5	AS	L	AS
6	L	L	L
7	AS	L	AS
8	L	AS	AS
9	L	L	L
10	L	AS	AS

Key:	
AS	*Active supporter*
L	*Primary leader*

[109] Stakeholders included service providers, network operators and equipment suppliers.

Recommendation Overview

The first five Recommendations deal primarily with robustness, while the remaining five deal primarily with availability - though each has some impact on both network aspects. Figure 10 provides a high level overview of the relationship of the Recommendations. Here a timeline is used to show the progressive situations of normal operation, crisis, recovery and return to normal operation. *Availability*, by definition, spans the entire timeline, but is most meaningful when understood in normal situations. On the other hand, *robustness* is concerned with times of stress, and thus is mostly applicable to the times of crisis.[110]

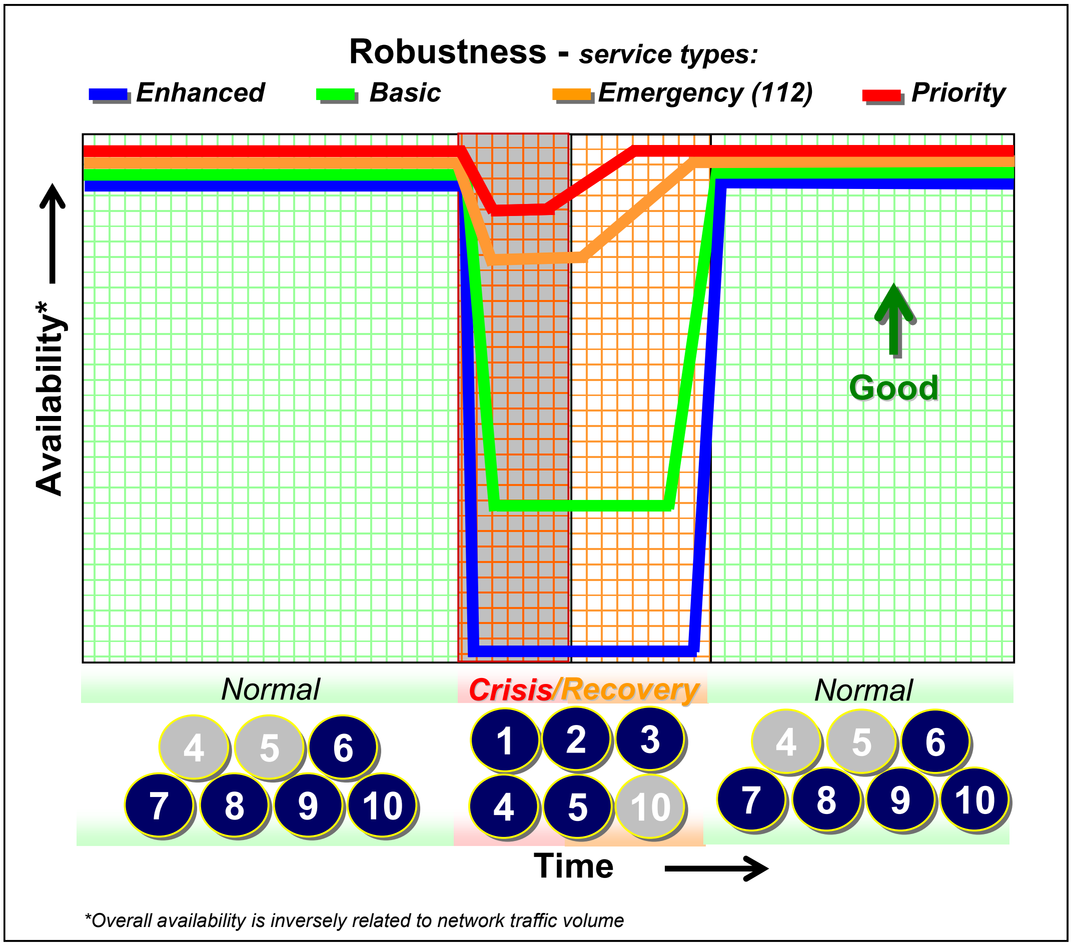


Figure 13: Impact of Recommendations in Relation to Infrastructure Stress Event

Continuing with reference to Figure 10, the following is a brief summary of the impact of each Recommendation.

- Recommendation 1, (**Emergency Preparedness**) reduces the duration of the recovery time.
- Recommendation 2 (**Priority Communications on Public Networks**) provides for priority communications service (i.e. the red line), or supplements an existing service over private networks with one built on public networks. It also extends the service capability to include inter-Member State and international service.

[110] See *Terms of Reference*, Section 2.2.1.

- Recommendation 3 (**Formal Mutual Aid Agreements**) maintains all types of services during a crises and the recovery period.
- Recommendation 4 (**Critical Infrastructure Information Sharing**) promotes service availability levels during crises and reduces the recovery interval. Also, during normal conditions, it can mitigate the occurrence or impact of future incidents.
- Recommendation 5 (**Inter-Infrastructure Dependency**) promotes robustness by reducing the recovery time after an incident and promotes availability by preventing or mitigating the impact of future incidents.
- Recommendation 6 (**Supply Chain Integrity and Trusted Operation**) promotes availability of all services.
- Recommendation 7 (**Unified European Voice in Standards**) promotes availability of all services.
- Recommendation 8 (**Interoperability Testing**) promotes availability of all services.
- Recommendation 9 (**Vigorous Ownership of Partnering Health**) promotes availability of all services.
- Recommendation 10 (**Discretionary European Expert Best Practices**) promotes availability of all services and can reduce the recovery time interval.

Relationship between Key Findings and Recommendations

The 100 Key Findings of Section 3 played a key role in the formulation of the Recommendations. After assembling the Key Findings, the Study team prioritised them, addressing both the availability and robustness aspects of the Study's mission equally. The team used its expertise in network reliability, network security, infrastructure protection and emergency preparedness to analyze the Key Findings to determine possible courses of action that could have the *maximum impact* on availability and robustness, the *readiness of industry and government* to support such actions and *alignment with the principles* that guided the Study throughout.[111] Figure 11 shows the number of Key Findings, grouped by maturity level, used by each Recommendation. This graphical representation provides an overview of the maturity levels involved and their relative proportion. One observation is that each Recommendation covers a range of maturity issues. This is usually because the presentation of the Recommendation includes both an assessment of the situation, which is wanting; and also includes the direction forward, which is a higher maturity level. Specific Key Finding references are integrated throughout the presentation of each Recommendation.

[111] *Principles of Approach*, Section 2.4. promote the interests of the citizens of Europe, be forward-looking, European focus, be inclusive of all insights, balanced representation, use competency to develop achievable objectives, fulfil the formal requirements.

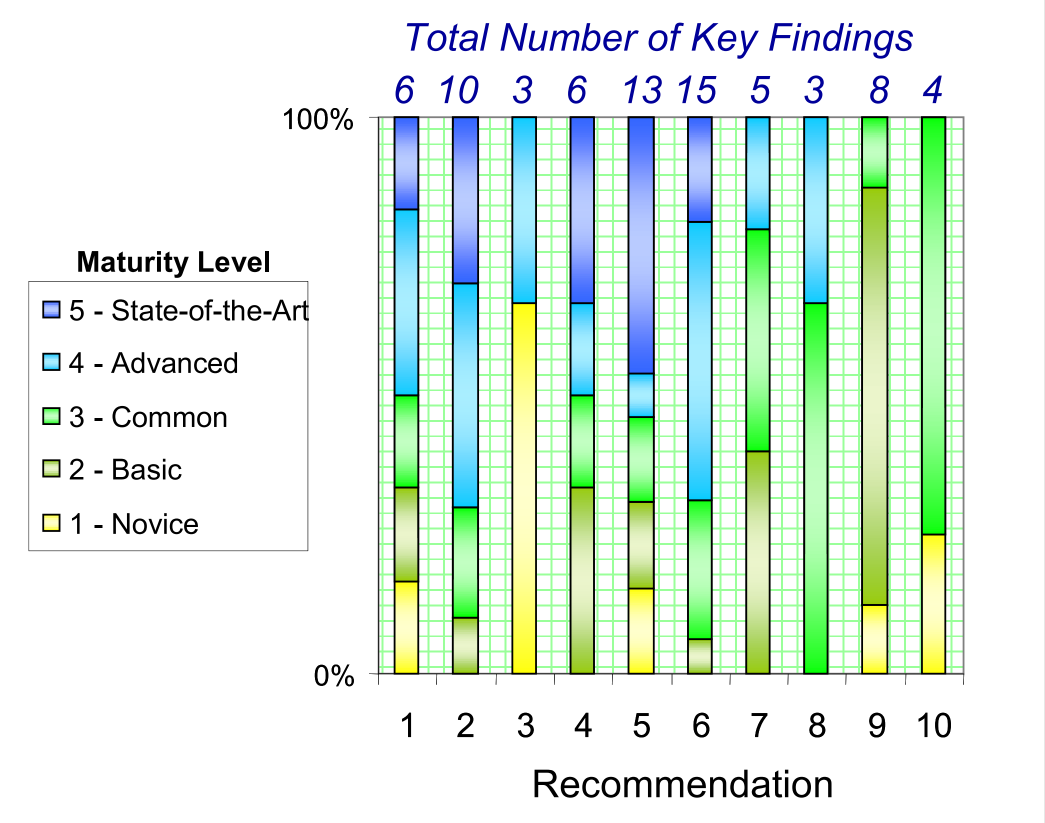


Figure 14: Recommendation References to Key Finding Maturity Levels

4.1 Emergency Preparedness

Background

Practice makes perfect. This old adage certainly applies to preparing for the inevitable emergency situations that face critical infrastructure stakeholders.[112,113] *While some network operators, service providers and government stakeholders do conduct periodic emergency preparedness exercises, others have made very limited investment in this area.*[114, 115, 116] *In many cases, most often with new entrants, the preparedness plans are mostly informal and lack structure.*[117] *The increased interconnectedness of European future networks can propagate the negative effects of weak preparedness from one provider to others. While industry experts are split on their opinion of their specific organisation's ability to deal with emergencies, they are much less confident on other organisations' ability to deal with emergencies. In summary, the effort expended in preparing for disasters is too often insufficient; disproportionate in relation to the critical services (public safety, economic, nation-state security) that depend on it, lacking involvement of respective Member State governments and coordination at a regional or European level, and bereft a formal prioritised restoration scheme.*[118]

Recommendation 1
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.

Required Commitments

To sustain the viability of this Recommendation, the Private Sector, Member States and European Institutions must be committed to defined courses. Specifically,

(a) The Private Sector must conduct emergency exercises,[119] first within its own organisations and then including multiple organisations within the industry, including organisations that might not previously have been considered as critical infrastructure.[120, 121]

(b) Member State governments and European Institutions must be willing to support Private Sector exercises and commit the resources necessary to efficiently interface with network operators and service providers during a crisis.

(c) The Private Sector and Member State Governments must conduct emergency exercises that include additional infrastructures and actively

[112] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 6, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[113] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 2, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[114] Key Finding 18, The level of emergency preparedness varies greatly across Europe, Section 3.2
[115] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 3, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[116] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 7, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[117] Key Finding 3, Emergency Preparedness is largely informal, Section 3.1.
[118] Priority restoration of communications circuits was critical for the Wall Street Financial District following the September 11, 2001 terrorist attacks.
[119] Key Finding 60, Emergency exercises are essential in preparing for disasters, but are not being sufficiently utilised, Section 3.4.
[120] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 10, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[121] International CIIP Handbook 2006, Volume II, "Sectors and Beyond: Analyzing what is Critical" page 31, Center for Security Studies, ETH Zurich.

address the interdependency issues that exist between various infrastructures.

(d) The Private Sector and Member State governments (and European Institutions for regional events) must jointly convene analysis groups following emergency incidents to study the response to those incidents, identify key learnings, and modify emergency response plans based on those learnings.

(e) The Private Sector and Member State and European Institution governments must identify critical services and develop formal plans, including removal of legal barriers if necessary, for providing priority restoration to those services during crisis situations.[122]

Purpose

This Recommendation is aimed at *improving the speed of response* to crisis situations by making as many decisions as possible before the crisis occurs. If implemented, its impact will be to *strengthen infrastructure robustness* by better preparing for unknown stress conditions and *improving network availability* by reducing the time required to restore services.

Benefits of Emergency Preparedness Planning

Planning and preparing for the inevitable emergency are the hallmark of a quality organisation. Being the infrastructure on which other infrastructures depends compels the communications industry to make preparation for emergencies to ensure rapid recovery following a disaster. Practicing emergency procedures prior to an incident reduces the number of decisions that must be made during an actual emergency, and improves both the speed and quality of the decisions that are made. In addition, pre-arranging priority restoration with other infrastructures (e.g., electric power[123]) improves the availability of communications services,[124] and identifying specific customers (e.g., police, fire, health care) for priority restoration improves the efficiency with which critical public services are restored.

Alternative Approaches and Their Consequences

- Informal disaster recovery plans . . . *take additional time to implement when disaster strikes.*
- Simple, unrealistic emergency drills . . . *leave the individuals charged with executing the plan unprepared and unpractised.*
- Interfaces with other infrastructures based on personal contacts . . . *result in single points of failure should the personal contact be unavailable.*
- Decisions on priority restoration made after the disaster happens . . . *requires additional decision making during the crisis, delaying restoration or resulting in restoration activity without priority.*

Next Steps

Suggested next steps to generate momentum toward the implementation of this Recommendation include:

1-1. The Private Sector and Member State governments should jointly convene to review recent emergency situations and stakeholders' response to those situations, and develop a list of lessons learned, to be shared with all participants.

[122] Key Finding 29, Priority restoration for critical subscribers is not commonly supported, Section 3.3.

[123] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 11, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[124] Key Finding 59, Critical communications infrastructures lack priority restoration agreements, Section 3.4.

1-2. The Private Sector and Member State governments should jointly conduct periodic emergency exercises that include multiple members within the industry, other infrastructures, and multiple Member States.[125]

1-3. Member State governments and the Private Sector should meet to review current regulations that may govern priority restoration, and develop a formal plan for pre-identifying critical services and providing priority restoration for those services.

Measures of Success

The successful implementation of this Recommendation can be gauged by the following measures:

> **Communications sector emergency exercises:** Periodic emergency exercises, involving multiple organisations that provide critical communications infrastructure, are conducted, simulating actual conditions and measuring the stakeholders' coordinated response.
>
> **Cross-infrastructure emergency exercises are conducted:** Emergency exercises are conducted with multiple infrastructures, and with multiple countries.
>
> **Priority restoration procedures are established:** Formal agreements with other infrastructures are established to provide priority restoration of services (e.g., power) required to maintain communications infrastructure.[126] In addition, customers with priority restoration needs (e.g., police, fire, health care) are identified.
>
> **Post incident lesson learned studies conducted:** Following emergency incidents, involved industry and government members meet to determine what procedures worked, and what procedures need to be created or modified to improve the speed of recovery. This includes European Institutions for incidents affecting multiples Member States.

[125] Key Finding 84, Disaster recovery arrangements across national boundaries are limited, Section 3.5.

[126] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 9, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

4.2 Priority Communications[127] on Public Networks

Background

During disaster situations, whether natural or manmade, certain communications are simply essential for saving lives and property as recovery occurs.[128] *First responders and other government authorised users entering the area need to be able to effectively communicate with each other, with other agency responders in the theatre of operation and between the disaster area and the "outside." The more diverse communication tools that can be rapidly deployed during a disaster situation, the greater the probability to successfully address the communication challenges. Some responders may have their own self contained radios for communication within the local response team, but other staff and other agencies may rely on a private network for essential communications, especially between agencies. However, full advantage should be taken of the wireline, wireless, and IP access capabilities for maximum diversity when networks are adversely affected by a disaster. Public networks are in place and a priority scheme can be integrated into the architecture of future networks so that the public networks and the variety of access technologies can be used to extend emergency communications capabilities.*[129]

Recommendation 2

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.

Required Commitments

To sustain the viability of this Recommendation, the Private Sector, Member States and European Institutions must be committed to defined courses. Specifically,

a) The Private Sector, European Institutions and Member States must work together as equal, trusted partners to ensure the proper focus and level of effort for these initiatives.

b) The Private Sector and Member States must participate in future network standards bodies to ensure that the requirements developed by these bodies meet all the unique needs of the Member States.

c) European Institutions must facilitate the interoperability of a priority communications capability that spans Europe and supports interoperability with the international community.[130]

d) As primary stakeholders for such a capability, Member State governments must fund its development, implementation and ongoing maintenance.[131]

e) The Private Sector must develop, deploy, and implement the emergency services as they become incrementally defined by the various standards bodies.

[127] Priority calling is defined as a government authorised caller placing a call that is marked as priority by the network and given preferential treatment to increase its probability of completion (also known as authority-to-authority calls).

[128] Key Finding 28, Priority calling for critical communications in public networks is needed. Section 3.3.

[129] Key Finding 56, IP-based emergency communications services have not been deployed. Section 3.4.

[130] Key Finding 86, Priority communications mechanisms are needed between Member States. Section 3.5.

[131] Key Finding 6, The deployment of priority communication services is awaiting government funding Section 3.2.

Purpose

This Recommendation addresses the issue of *how to maximise the probability that the most essential communications are completed during periods of high traffic*. This capability focuses on the aspect of robustness that retains the most critical functions during periods of stress.

Benefits of Priority Calling on Public Networks

Many countries have separate emergency networks to support leaders, military, and other authorised users.[132] While these networks have proven valuable and should be maintained, an emergency scheme[133] on future public networks is also needed to supplement these private networks.

It is desirable to include placing or receiving priority calls from stations that are not connected directly to the private network and are only present on the public network. In addition, if the private network becomes overloaded or otherwise unavailable (e.g., physical damage or an exploited software vulnerability), having a priority capability on future public networks provides a second mechanism for achieving the priority communications needed by a Member State or across Member State boundaries for the emergency situation.[134]

Achieving priority on future networks will be more challenging than on a legacy network due to the complexity of bandwidth management,[135] the various types of services supported[136, 137] and the authorisation issues.[138]

Alternative Approaches and Their Consequences

- Priority calling is not offered on public networks . . . *means key stakeholders are unable to (a) originate a priority call when not on the private network or (b) terminate a priority call to critical people not on the private network.*
- Priority calling is only offered on private networks . . . *results in priority calling being unavailable when the private network is comprised or impaired.*
- Member States focus only on priority calls within their national boundaries . . . *means that priority calling between Member States will be unavailable on the public network*

Next Steps

Suggested next steps to generate momentum toward the implementation of this Recommendation include:

2-1. Member States to create and provide specific mission based needs[139] descriptions for priority calling.

[132] Key Finding 85, Several Member States have completely separate communications networks for critical functions. Section 3.5.

[133] Key Finding 51, Net Neutrality may be misunderstood. Section 3.3.

[134] Key Finding 87, Validation of user authorisation to place priority emergency calls does not address inter-network calls. Section 3.5**.**

[135] Key Finding 64, Many network operators do not prioritise packets. Section 3.4.

[136] Different session types require different classes of sessions. The priority mechanism must address both the establishment of the session as well as the individual payload packets of the session to maintain QoS. Each type of traffic may have different QoS and transport characteristics that must be allowed for in the priority mechanism. While the initial application is voice, data and video functions will follow shortly, so the scheme should be designed to effectively address these multiple classes of service from the beginning to avoid additional costs and disruptions that would naturally occur if the requirements are only addressed incrementally.

[137] Key Finding 57, Future networks have the opportunity to introduce mechanisms for early warning services. Section 3.4.

[138] Key Finding 55, Authorisation of priority communications users must be managed. Section 3.4.

[139] The Member State governments are responsible for protecting the population during periods of crisis. As such the definitions of the specific capabilities needed to accomplish their mission must be specified by the Member

2-2. Private Sector and Member States convene for the purpose of agreeing on standards for priority calling on public networks.

2-3. Member States allocate funds for the deployment of priority calling over public networks.

2-4. Equipment suppliers implement the agreed priority calling functionality in their products.

2-5. Private Sector network operators deploy priority calling features in their networks.

Measures of Success

The successful implementation of this Recommendation can be gauged by the following measures:

> **Needs Defined:** Member State mission based needs are clearly defined and provided to standards bodies.
>
> **Standards Developed:**[140] A priority calling standard has been developed that includes unique European needs.
>
> **Member State Agreements:** Member States have agreed to deploy the priority calling standards.
>
> **Member State Funding:** Member States have allocated funds for the deployment of priority calling.
>
> **Priority calling deployed**: Priority calling has been deployed on public networks within the Member States.[141]
>
> **Inter-Member State priority calling deployed:** Priority calls between Member States' networks are supported.

States. These definitions can then be used to create the priority calling standards with the assurance that the end product is consistent with the government's mission.

[140] European stakeholders participated in the creation of the standards and are comfortable that it meets European needs.

[141] This includes the establishment and maintenance of national authorisation databases.

4.3 Formal Mutual Aid Agreements

Background

The enterprises that comprise the critical infrastructure of Europe are fiercely competitive, as is appropriate in a free market economy. They can best serve the public by tending to their own networks and maximizing the return on their investment. However, as citizens of the European community they also suffer when the critical infrastructure that serves the community is imperilled during a crisis, either natural or man-made. At these times, given the vital nature of communications networks, the greater well-being of society and the restoration of communications services outweigh individual business interests. Mutual aid between companies can greatly extend the robustness of their networks for a relatively low cost.[142] *However, while there are some few exceptions, mutual aid in Europe is not widely practiced.*[143] *Further, when mutual aid is practiced, it is largely ad hoc and susceptible to failure – especially during times of stress.*[144, 145]

Recommendation 3
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.

Required Commitments

To sustain the viability of this Recommendation, the Private Sector, Member State and European Institution governments must be committed to defined courses. Specifically,

(a) Private Sector service providers, network operators and equipment suppliers must acknowledge and accept their reasonable responsibility for maintaining critical services that directly impact social well-being and national security.

(b) The Private Sector must be willing to offer resources to help competitors in times of crisis.

(c) Service providers and network operators must consider executing mutual aid agreements with a wide range of industry participants, including non-traditional entities that comprise the European critical infrastructure.[146]

(d) Government powers (especially local governments) must provide communications workers with priority access to disaster sites during crisis situations and assistance in procuring and moving necessary materials (e.g., fuel).[147]

(e) European Institution and Member State governments must encourage industry cooperative efforts by removing legal barriers to mutual aid for crisis situations.

[142] Companies that establish formal mutual aid agreements are able to make use of a wide range of "back-up" equipment only when they need it, and avoid the costs of its purchase and maintenance.
[143] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 6, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[144] Key Finding 3, Emergency preparedness is largely informal, Section 3.1
[145] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 8, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[146] Key Finding 4, Future network operators may not be recognised as part of the critical infrastructure, Section 3.1.
[147] A key finding of the U.S. industry experience with the September 11, 2001 terrorist attacks and the 2005 Hurricane Katrina New Orleans Flood was that emergency access to these disaster sites by communications company technicians was vital to the recovery services.

Purpose

This Recommendation addresses the issue of *how to significantly extend the robustness and resiliency of any given network through the shared resources of other industry stakeholders.*

Benefits of Formal Mutual Aid Agreements

The nature of disasters is such that one network is often impaired more than another. The restoration of the former can be greatly assisted by the resources of the later. Examples include portable generators, fuel, personnel, or specific network equipment. In these situations, it may be in the best interests of the pubic – and individual companies, for competitors to work together. A formal, well planned agreement, entered into voluntarily as part of emergency preparedness and business continuity planning, fosters swift and coordinated responses to disaster situations and takes advantage of the combined strengths of stakeholders to further the public good.[148] While these agreements are not legally binding in terms of requiring a participant to give up resources, nor do they necessarily suggest that offered assistance is free, they do provide a framework that can expedite the emergency assistance process. Formal mutual aid agreements provide a low cost option for strengthening the robustness of any given network in a competitive environment.

Alternative Approaches and Their Consequences

- Stakeholders fend for themselves . . . *resulting in higher industry costs to adequately prepare for disasters, or inadequately prepared stakeholders.*
- Informal agreements between stakeholders . . . *take additional time to implement when disaster strikes.*
- Agreements based on personal contacts . . . *result in single points of failure should the personal contact be unavailable.*
- Agreements with only traditional stakeholders . . . *exposes elements of future networks critical infrastructure to inadequate support in times of crisis.*
- Private Sector efforts without European Institution or Member State support . . . *may encounter regulations that encumber the mutual aid process – discouraging industry efforts, raising costs, and reducing the reliability of critical infrastructure.*

Next Steps

The implementation of this Recommendation can be accelerated by following these suggested steps:

3-1. The Private Sector should convene to establish the characteristics that should be part of a standard template for mutual aid.[149, 150] These discussions should be open to any stakeholder who provides critical infrastructure.

3-2. Member States and European Institutions should examine regulation under their influence or control to ensure that it does not impede mutual aid between competitors or across national boundaries during crisis situations.

3-3. Mutual aid scenarios should be incorporated into industry, national, and international disaster recovery exercises.

[148] Key Finding 58, Mutual aid agreements are essential for effective incident response, Section 3.4.

[149] The standard template, once complete is intended to be a starting point (i.e. it can be modified by users to suit their specific requirements and preferences).

[150] Examples of aspects of an agreement template include: lists of available equipment, services, network capacity, schedule of fees, 24-hour contact information, safety, confidentiality, and legal and liability framework.

Measures of Success

The successful implementation of this Recommendation can be gauged by the following measures:

Consensus Agreement on Template: A mutual aid template is established by consensus agreement of key industry stakeholders. Member State regulators representatives should also be involved to ensure that regulation encourages mutual aid between competitors, and across national boundaries.

Formal mutual aid agreements are signed: Formal mutual aid agreements between industry stakeholders are put in place.

Mutual aid agreements are exercised during crisis situations: Stakeholders that comprise the critical infrastructure work together during crisis situations, resulting in improved resiliency and reliability of the networks that serve the public.

4.4 Critical Infrastructure Information Sharing

Background

Market liberalisation has resulted in Private Sector ownership of the overwhelming majority of communications infrastructure. The responsibility of protecting this infrastructure resides with its owners. However without knowledge of potential threats, those owners may not be able to provide the most effective protection. Government, during times of crisis, can provide the Private Sector with assistance in protecting and restoring critical infrastructure, but they cannot provide this help without knowledge of where the problems exist. There are barriers in both the public and Private Sectors to sharing this type of information, owing to its sensitivity and a lack of coordination between the stakeholders.[151, 152] *For the most part, information sharing that does take place is ad hoc and occurs informally – the linkage can be easily broken with the absence of one key person.*[153] *This leaves European communications networks avoidably less robust. Sharing critical information will strengthen the robustness of the networks of all involved by providing warnings, advice, and improved preparedness. For example, sharing information before an incident can prevent or mitigate its impact, during an incident can speed up recovery and after an incident can facilitate the capture of important learnings to improve good practice.*

Recommendation 4

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.

Required Commitments

To sustain the viability of this Recommendation, Member States and the Private Sector must be committed to defined courses. Specifically,

(a) Private Sector enterprises that own critical communications infrastructure must jointly establish a *trusted environment* for sharing information to improve the protection and rapid restoration of that infrastructure.[154, 155]

(b) Private Sector service providers, network operators and equipment suppliers must be willing to share threat and outage information within a trusted environment within the industry for the common good.[156, 157, 158]

(c) Government authorities must be willing to share threat and other sensitive information with providers of critical communications infrastructure, and safeguard information related to critical infrastructure provided by industry.[159]

[151] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 8, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[152] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 3, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[153] Key Finding 19, Emergency information sharing during incidents is limited, Section 3.2

[154] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 7, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[155] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 2, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[156] The Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC) has documented strong industry-wide network reliability improvements based on industry voluntary collaborative initiatives that involve the sharing and analysis of outage information. ATIS NRSC 2003 Annual Report, September, 2004, www.atis.org/nrsc/annualrpt.asp..

[157] Key Finding 35, Dialogue within the industry is limited, Section 3.3.

[158] Key Finding 89, Collaboration between stakeholders in the U.S. is perceived to be more mature than in Europe, Section 3.5.

(d) Member State governments must be willing to share information that will improve the protection and rapid restoration of critical infrastructure with other Member States[160] as well as the providers of that infrastructure within those other Member States.

Purpose

This Recommendation addresses *the need to share sensitive information between industry and government stakeholders, within a trusted environment, enabling all participants to benefit from this shared body of knowledge.*

Benefits of a Formal Information Sharing Process

Knowledge is power. Sharing information among providers of critical infrastructure and the governments whose constituencies depend on that critical infrastructure, provides stakeholders with additional knowledge and insights to help them prepare for, and react to, attacks or incidents. The sharing of sensitive information will only occur and flourish in an environment characterised by openness, concern for the common good, and most of all, *trust*.

Stakeholders most experienced with effective information sharing emphasised the importance of getting the architectural model that best aligns with the interests of the parties invited to participate. For the set of interests discussed here, the model shown in Figure 12 (B) offers an option that may be welcome to the affected stakeholders. In contrast to a “star” arrangement where all sensitive information passes through a European Institution entity, the mesh network encourages information sharing directly between parties willing to share. By enabling sharing to thrive where trust exists, the end result will be substantially more information being shared.

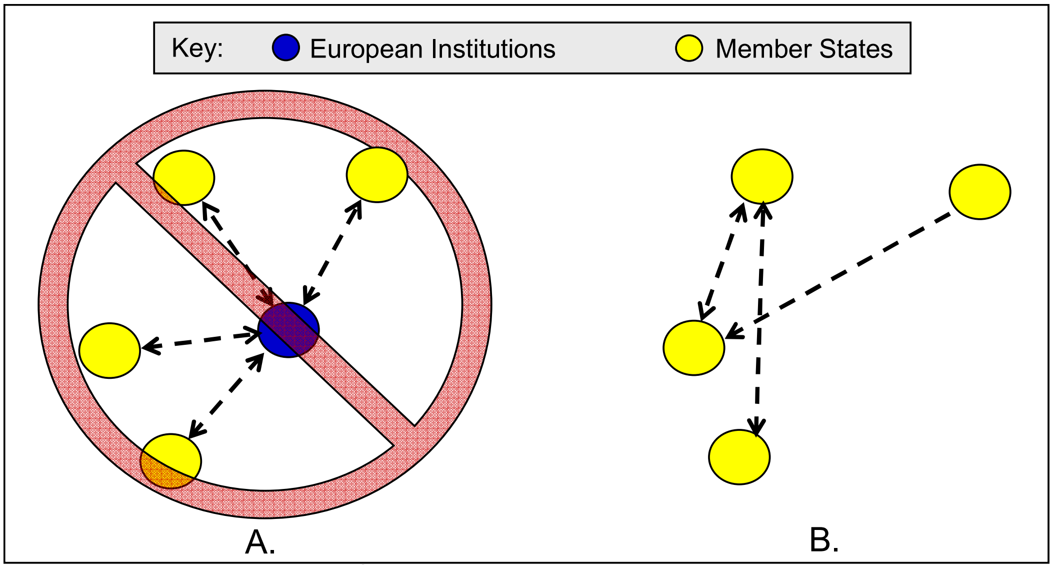


Figure 15: Star (A) and Mesh (B) Architecture Models

[159] Key Finding 19, Emergency information sharing during incidents is limited. Section 3.2.
[160] Key Finding 70, Information sharing of network security incidents with Member States is limited. Section 3.4.

Alternative Approaches and Their Consequences

- Industry stakeholders sharing only with selected partners . . . *resulting in fragmented sharing and response to attacks, and various providers of critical infrastructure being left uninformed.*
- Critical government information kept within government . . . *reduces industry's ability to prepare and respond to attacks.*
- Industry threat and outage information shared only within industry . . . *leaves government interests under-protected and eliminates potential benefits of government assistance during a crisis.*
- Information sharing kept within a Member State . . . *weakens the ability of other Members States to prepare and respond, and negatively impacts the reliability and security of all networks connected to those of the uninformed Members States.*
- A mandated environment for information sharing not built on mutual trust . . . *results in sharing only to the extent of the mandate, potential unintended consequences, and lost opportunity to benefit from a common body of knowledge.*
- Establishment of a European Institution level program *. . . resulting in loss of Member State control and less effective "star" architecture*

Next Steps

Relative to the other Recommendations, this one takes a considerably longer time to develop. This is because it is based on trust and the development of trust requires time – months and years. This is all the more reason for the initial steps to be taken without delay. The following suggested next steps can facilitate the implementation of this Recommendation and the building of that trust.

4-1. The Private Sector and Member State stakeholders should investigate, and where appropriate, join some of the excellent information sharing organisations that already exist,[161, 162, 163] learning their methods[164] and creating an even larger pool of knowledge, mutually benefiting all organisations.

4-2. The Private Sector and the Member State stakeholders should convene to establish a trusted environment for information sharing within each Member State, identifying the owners of critical infrastructure, the key stakeholders and the type of information that will be shared, both from industry to government and from government to industry.

4-3. Member States governments should identify those information sharing models which will best enable the sharing of threat and other sensitive information across Member State boundaries. These models should be implemented, if they do not already exist, and this information should then be shared, as appropriate, with industry partners within those Member States.

Measures of Success

The successful implementation of this Recommendation can be gauged by the following measures:

[161] Key Finding 98, Europe has positive information sharing role models, Section 3.5.
[162] NISCC, www.niscc.gov.uk/niscc/index-en.html.
[163] International CIIP Handbook 2006, Volume I, "Information Sharing and Analysis Centres (ISAC)" page 329, Centre for Security Studies, ETH Zurich.
[164] WARPS, www.warp.gov.uk.

Establishment of information sharing forums within Member States: Individual Member States and industry members who operate within those Member States establish a trust-based forum for information sharing.

Implementation of an information sharing model across the European Union: Member State governments and industry stakeholders establish a trust-based forum for bi-directional information sharing.

New entrants to the communications industry seek membership in the trusted forums: New entrants to the industry, along with organisations that may not normally be considered part of the industry, begin seeking membership in the information sharing forum to avail themselves of its benefits.

4.5 Inter-Infrastructure Dependencies

Background

Critical infrastructures, which play a major role in the economic, physical and cyber well-being of Europe, form a complex "system of systems." Critical infrastructure protection is at varying stages of being addressed in the Member States[165, 166] and the European Institutions.[167] Interdependencies are complex and need to be understood since disruptions in one infrastructure can propagate into other infrastructures. While specific critical infrastructure protection and recovery responsibilities are primarily local[168, 169] they may have a European-wide impact.[170]

Recommendation 5

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.

Required Commitments

To sustain the viability of this Recommendation, the Private Sector, European Institutions and Member State governments must be committed to defined courses. Specifically,

(a) Communications service providers and network operators need to recognise their interdependencies with other critical sectors[170,171] and appropriately support efforts to better understand and manage those interdependencies.

(b) The Private Sector, European Institutions and Member States must continue to work together to understand and develop their specific roles to ensure the proper focus and level of effort and coordination for these initiatives.[172, 173, 174]

(c) European Institutions and Member State governments must be willing to fund research to address aspects of interdependencies insufficiently understood.

(d) The research community must provide solutions to substantially strengthen the understanding of critical sector interdependencies and enable effective management of complex and dynamic interactions.[175]

[165] International Critical Information Infrastructure Protection Handbook 2006, Volume 1, "An Inventory of 20 National and 6 International Critical Infrastructure Protection Policies," Center for Security Studies, ETH Zurich.

[166] International Critical Information Infrastructure Protection Handbook 2006, Volume 2, "Analyzing Issues, Challenges, and Prospects," Center for Security Studies, ETH Zurich.

[167] Green Paper, On a European Programme for Critical Infrastructure Protection, Commission of the European Communities, COM(2005) 576 final, Brussels, BE, 17 November 2005.

[168] Key Finding 40, Agreements, standards, policies and regulations (ASPR) are Member State dependent, Section 3.3.

[169] Key Finding 41, Local governments play a critical role in maintaining the reliability and security of networks, Section 3.3.

[170] 2006 European Experts Workshop on Power & Environment, Top Concerns 3, 5, 11, , slides 10, 12, 15, (www.comsoc.org/~cqr/EU-Proceedings-2006).

[171] Key Finding 4, Future network operators may not be recognised as part of the critical infrastructure. Section 3.1.

[172] Key Finding 89, Collaboration between stakeholders in the U.S. is perceived to be more mature than in Europe. Section 3.5.

[173] 2006 European Experts Workshop on Power & Environment, Top Concern 13, , slide 10, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[174] 2006 European Experts Workshop on Policy & Human, Top Concern 16, slide 18, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

Purpose

This Recommendation is aimed at *enhancing the availability and robustness of Europe's critical infrastructures by identifying and addressing sector interdependencies*.

Benefits of Addressing Inter-Infrastructure Dependencies

Effectively addressing sector interdependencies is essential to enhancing critical infrastructures availability and robustness. Critical infrastructures may be subject to communications disruptions, such as

- *Communications Sector:* congestion or disruption of key communications nodes[176, 177] (e.g., due to fire, wind, water, sabotage, terrorism).
- *Power Sector:* blackouts caused by SCADA outages preventing sufficient generation to meet demand or preventing control to eliminate transmission bottlenecks or cascading power outages.
- *Emergency Services Sector:* demand for emergency services can exceed the communications network capacity during a disaster.[178]
- *Banking and Finance Sector:* communications disruption of electronic payments systems causes bank liquidity problems or inability to make business-critical and cash machine transactions.

Alternative Approaches and Their Consequences

The following alternatives are less desirable approaches:

- Ignoring interdependencies that cross national boarders . . . *will miss interdependencies, lower availability and robustness of each infrastructure and negatively impact the economy, health and safety of the people served by those infrastructures*.
- Member State or European regulation that is not produced with industry and cross-sector collaboration . . . *resulting in unintended consequences*.
- Taking no action . . *. may result in magnified, cascading outages* ***within*** *sectors (e.g., multi-national regional power outages) and* ***across*** *sectors (e.g., power outage causing telecom outages).*

Next Steps

5-1. Member State governments should engage the Private Sector to

A. systematically identify the existing interdependencies between critical sectors,[179, 180] including those crossing national boundaries

B. prioritise each of these interdependencies

C. create a functional map[181, 182, 183, 184, 185] of the critical aspects[186] of the highest priority interdependencies in order to better prepare for, and mitigate against, the impacts of a natural or manmade threat

[175] This was clear from all of the work shops and many of the Key Findings that all discussed the complexity of the problems, the dependencies and the numerous gaps. For example, Key Finding 37, Feature interoperability between legacy networks and new networks is complex. Section 3.3.

[176] Key Finding 84, Disaster recovery arrangements across national boundaries are limited. Section 3.5.

[177] Key Finding 91, Minimal network management information is shared between broadband network operators and access service providers. Section 3.5.

[178] Key Finding 86, Priority communications mechanisms are needed between Member States. Section 3.5.

[179] Key Finding 92, There is minimal information sharing between critical sectors. Section 3.5.

[180] Key Finding 98, Europe has positive information sharing role models. Section 3.5.

[181] 2006 European Experts Workshop on Hardware & Software, Top Concerns 16, 33, slides 13, 15, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[182] 2006 European Experts Workshop on Policy & Human, Top Concern 23, slide 18, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[183] 2006 European Experts Workshop on Power & Environment, Top Concern 9, slide 10, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

5-2. European Institutions and Member State governments should fund research for developing modelling methodologies for better understanding the dynamic and cascading aspects of dependencies inherent within Europe's critical infrastructures.

5-3. European Institution and Member State governments should jointly[187,188,189] identify regulatory issues, which if addressed, may reduce interdependencies between infrastructures.

Measures of Success

The successful implementation of this Recommendation can be gauged by implementation of the following measures:[190, 191]

Interdependencies identified: To what degree have the existing interdependencies (including those that cross national borders) been identified?

Interdependencies prioritised: To what degree have the interdependencies been prioritised?

Functional map: Have the critical aspects of interdependencies been mapped?

Research funded: Has government funded research to develop a better understanding of dynamic and cascading aspects of dependencies.

[184] Key Finding 19, Emergency information sharing during incidents is limited. Section 3.1.

[185] Key Finding 59, Critical communications infrastructures lack restoration agreements. Section 3.4.

[186] For example, ownership, 24-hour emergency contact information, expectations for restoral procedures, priority restoration programs, incident reporting procedures.

[187] Key Finding 26, The Private Sector is not treated by government as an equal partner. Section 3.2.

[188] 2006 European Experts Workshop on Policy and Human, Top Concern 7, slide 17, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[189] 2006 European Experts Workshop on Policy & Human, Top Concern 28, slide 19, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[190] 2006 European Experts Workshop on Policy & Human, Top Concern 14, slide 18, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[191] Key Finding 25, Companies are not committing appropriate expertise in engagements with the government. Section 3.2.

4.6 Supply Chain Integrity and Trusted Operation

Background

Integrity and trust are essential to building and operating communications networks. For future ICT networks, managing and securing the network elements will be significantly more challenging than today, requiring the implementation of supply chain trust concepts for both hardware and software.[192, 193] *Future networks will consist of many more network elements*[194] *with many of these elements consisting of outsourced components supplied by both new and established equipment suppliers.*[195] *Many of these components will utilise common hardware and software modules, thereby increasing the potential for single modes of failure or cascading network problems.*[196] *Further, ensuring the end-to-end security of future networks*[197] *will increasingly rely on innovative concepts such as trusted relationships not only between service providers, but also between network elements, applications and end-user devices.*[198, 199] *Existing solutions are not sufficient to address the challenges of future networks.*[200, 201] *New technologies will be required to enable innovative solutions to these problems.*

Recommendation 6

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.

Required Commitments

To sustain the viability of this Recommendation, the Private Sector, and European Institution and Member State governments must be committed to defined courses. Specifically,

(a) European Institutions and Member States should articulate a vision that properly stresses the importance of trusted hardware, software and networks.

(b) European Institutions and Member States should encourage, by policy and economic incentive, research that supports the development and implementation of supply chain processes and safeguards that provide assurances for technology trustworthiness.

(c) European Institutions and Member States should provide incentives for Private Sector investment by awarding government communications services contracts to those service providers most aligned with these principles to improve security and effectively address intrinsic vulnerabilities.

(d) The Private Sector needs to continuously pursue technology improvements in the quality and control of their supply chains across

[192] Key Finding 17, Layered software introduces additional complexity, Section 3.2.
[193] Key Finding 76, Third party components may have an adverse impact on networks, Section 3.4.
[194] Key Finding 39, Future networks will be more difficult to manage, Section 3.3.
[195] Key Finding 77, New equipment vendors may have an adverse impact on the supply chain, Section 3.4.
[196] Key Finding 80, Cascading failures of a hardware component or a software element require new management strategies, Section 3.4.
[197] Key Finding 96, End-to-end security is implemented hop-by-hop, Section 3.5.
[198] Key Finding 79, Introduction of network security may impact service availability, Section 3.4.
[199] Key Finding 75, Future networks are more vulnerable to signalling fraud from end-user devices, Section 3.4.
[200] Key Finding 43, Security approaches used by the PSTN/IN are not sufficient for future networks, Section 3.3.
[201] Key Finding 95, Future networks co-mingle control messages with normal subscriber traffic, Section 3.5.

the product lifecycle to increase the security assurance of information and communications systems.

Purpose

This Recommendation is aimed at *providing hardware and software supply chain technology and assurances of integrity* regardless of where or by whom the technology was designed, developed, manufactured, or deployed. It is further aimed at *operating future networks with safeguards that provide assurances of trustworthiness*, regardless of their owner or operator.

Benefits of Supply Chain Integrity and Trusted Operations

Flaws introduced either deliberately or unintentionally can occur across the entire technology lifecycle (i.e. design, development, test, deployment and support). The current trend by equipment suppliers and service providers to leverage the advantages of outsourced and offshore mechanisms may present increased risk because there are few broadly-used standards, mechanisms, controls, or capabilities for lifecycle quality assurance.

Future networks, characterised by a large number of widely distributed and powerful hardware and software components, raise the importance of trustworthiness and security assurance. The reliability and security of networks are complicated by the increased diversity of vendors, and by services delivered by an increasing number of providers; these vendors and providers will have varying levels of competency and discipline relative to security.

While the Private Sector is ultimately responsible for the integrity of supply chains and implementation of trusted technologies, government assistance can facilitate a uniform industry approach by providing incentives for research and by awarding contracts to parties demonstrating leadership and the necessary proficiency. Government advocacy for supply chain integrity and operational trustworthiness is appropriate because the levels of security and reliability required to protect the government’s interests, such as nation-state security and economic stability, exceed that of the bulk of the commercial market (Figure 13).

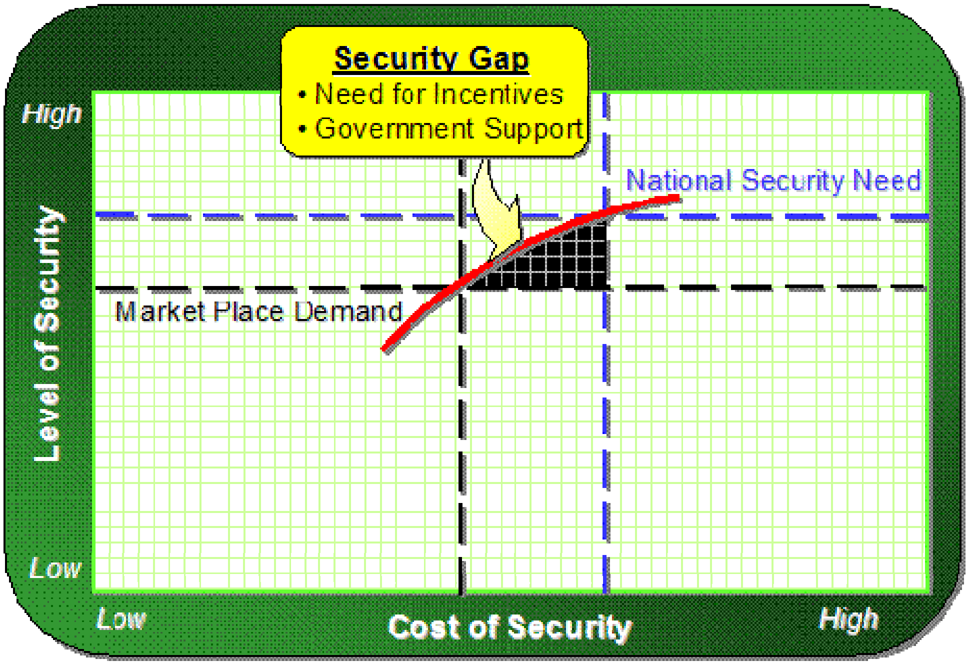


Figure 16: Nation-State Security Needs Exceed Market Place Demands[202]

Alternative Approaches and Their Consequences

- Indifferent government policies concerning integrity of critical network systems and their operation . . . *will result in inconsistent attention to security by network providers.* [203, 204]
- Government mandates on the Private Sector to prescribe aspects of network design or operation . . . *will fall short of appreciating this sector's complexity, evolving technology, and diversity of business approaches and likely deliver unintended consequences.*
- Continuing on the current course with inconsistent approaches to maintaining the integrity of supply chains, and with an inconsistent approach to providing trust . . . *will likely result in suboptimal network availability and robustness for future European networks*.[205, 206, 207, 208]

Next Steps

Suggested steps to begin the implementation of this Recommendation include the following:

6-1. European Institutions and Member States should articulate a vision that properly stresses the critical role of protecting supply chains and implementing operational trust-based programs.

[202] NRIC VI Homeland Security Physical Security Final Report, "Meeting NS/EP Security Needs", Issue 3, December, 2003, p.15.
[203] Key Finding 97, Reliability and security practices vary considerably across network operators and service providers, Section 3.5.
[204] Key Finding 74, Federated Identity Management will become a compelling security strategy in future networks, Section 3.4.
[205] Key Finding 50, Future networks contain signalling elements whose failure can cause major outages, Section 3.3.
[206] Key Finding 44, Future networks creates signalling traffic security and reliability challenges, Section 3.3.
[207] Key Finding 67, Future networks provide wider access to network controls, Section 3.4.
[208] Key Finding 71, Security standards are inconsistently implemented, Section 3.4.

6-2. European Institutions, Member States and the Private Sector should work together to establish appropriate criteria to evaluate the integrity of systems and trustworthiness of networks.

6-3. The appropriate entities within European and Member State governments should drive meaningful policy changes that focus public sector research, motivate academic research, and encourage Private Sector research and development of trusted technologies.

6-4. The appropriate entities within European and Member State governments should provide incentives to invest in trusted technology research.

6-5. The appropriate entities within European and Member State governments should drive meaningful policy changes that impact the awarding of contracts based on the successful implementations of these capabilities.

Measures of Success

The successful implementation of this Recommendation can be gauged by the following measures:

Vision Established: European Institutions and Member States have established and articulated a vision for protecting the supply chain and implementing trust-based programs.

Criteria Established: European Institutions and Member States have established evaluation criteria with the consensus support of industry subject matter experts.

Research: The appropriate academic and research entities have been funded to research and develop supply chain processes and safeguards that provide trustworthy assurances for technology.

Expertise Engaged: Industry expertise has been engaged to pursue technology improvements in the quality and control of their supply chains across the technology lifecycle.

Technology Deployed: Trusted technologies are implemented at network interfaces to provide end-to-end security.

4.7 Unified European Voice in Standards

Background

Standards are one important component of the broader category of ASPR (Agreements, Standards, Policy and Regulations)[209]*, sometimes referred to simply as "policy." As with hardware, software and networks, ASPR have intrinsic vulnerabilities, each of which provides opportunities for problems that can lead to outages. The complete list of intrinsic vulnerabilities include:*

- *Lack of ASPR*
- *Conflicting ASPR*
- *Outdated ASPR*
- *Unimplemented ASPR (complete or partial)*
- *Interpretation of ASPR (mis- or multi-)*
- *Inability to implement ASPR*
- *Enforcement limitations*
- *Boundary limitations*
- *Pace of development*
- *Information leakage from ASPR processes*
- *Inflexible regulation*
- *Excessive regulation*
- *Predictable behavior due to ASPR*
- *ASPR dependence on misinformed guidance*
- *ASPR ability to stress vulnerabilities*
- *ASPR ability to infuse vulnerabilities*
- *Inappropriate interest influence in ASPR*

While the standards bodies attempt to coordinate their deliverables, there remains the valid concern that incompatibilities of different standards,[210] *or releases of standards,*[211] *can cause communications to fail or to not work as expected.*[212] *On the positive side, there is a correlation between network reliability and the maturity of standards development and implementation. Thus, improving the maturity of industry standards can enhance network availability and robustness.*

Historically, there have been multiple standards bodies and often there is considerable overlap in their scope. Often the reasons different standards bodies overlap or duplicate scopes are political rather than technical. Member States may have a vested interest in national companies that do not want to adopt a competitor's standards from another country.

Many standards bodies have members representing Member States, private companies and some, such as the Internet Engineering Task force (IETF) have participants speak as individuals (although they have organisations or companies behind them). It is exactly at such forums as the IETF where the recommendation to have many voices support the aspects needed for the unique needs of the European Union member will be most productive. An added challenge is for the Member States not only to coordinate their own voices but to also encourage the respective operating companies and their equipment vendors to actively add their voices in support of the voices of the representatives of the Member States in the various standards bodies.

[209] Key Finding 40, Agreements, Standards, Policies and Rules (ASPR) are Member State dependent. Section 3.3.

[210] Key Finding 7, Multiple standards bodies are producing different standards. Section 3.2.

[211] Key Finding 13, Future networks require vigilance in upgrading software. Section 3.2.

[212] Key Finding 37, Feature interoperability between legacy networks and new networks is complex. Section 3.3.

Recommendation 7
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.

Required Commitments

To sustain the viability of this Recommendation, the Private Sector, Member States and European Institutions must be committed to defined courses. Specifically,

(a) Member States and Private Sector service providers, network operators and equipment suppliers will need to embrace the need to establish standards that will benefit the European communications industry as a whole.

(b) Member States, with the active support of private industry, should represent its constituents with one voice to increase the joint influence of the European communications community

Purpose

This Recommendation is aimed at *promoting network availability by reducing conflicts between network operators, service providers, equipment suppliers, and between networks operating across Member States' boundaries by adopting common standards*.[213]

Benefits of Unified European Voice in Standards

Coordination at standards bodies strengthens the European Union influence and ensures that the standards meet the needs of the European community.

Alternative Approaches and Their Consequences

- Member States participate in standards bodies independently . . . *resulting in European interest not being represented as strongly as possible.*
- Member States adopt different standards . . . *resulting in operational conflicts on communications sessions that cross Member State boundaries. These conflicts will have to be discovered and resolved as they occur.*

Next Steps

Suggested next steps to generate momentum toward the implementation of this Recommendation include:

7-1 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.

7-2 Member States and Private Sector service providers, network operators and equipment suppliers should actively participate in the agreed upon standards bodies, coordinating their efforts to ensure that all of the Member States' unique needs are addressed and resolved.

[213] Key Finding 61, Security integration and interoperability testing guidelines are inconsistent. Section 3.4.

Measures of Success

The successful implementation of this Recommendation can be gauged by the following measures:

Standards developed: The standards that are being developed meet the unique needs of the Member States.

Equipment deployed: Equipment based on uniform standards is being deployed in the Member States.

4.8 Interoperability Testing

Background

The procedures for determining the viability of new networks before interconnecting to existing networks are inconsistently defined by each interconnecting network provider.[214] *This is a potential source of conflict between network operators. Allowing interconnection without any testing would be imprudent for the network operators. Having non-uniform or capricious requirements leads to additional effort to accomplish such tests, as well as disputes about the results of the tests and the significance of any discrepancies*

Recommendation 8

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.

Required Commitments

To sustain the viability of this Recommendation, the Private Sector, Member States and European Institutions must be committed to defined courses. Specifically,

(a) The Private Sector must embrace the need for a standardised network-to-network testing framework.

(b) Member States must recognise a standardised testing framework as a reasonable means for determining the readiness of networks to be interconnected.[215]

Purpose

This Recommendation is aimed at *enhancing the reliability of future networks by establishing an agreed upon set of tests that would be executed prior to the connection of a new network to existing networks*.[216] This testing framework will help to ensure the integrity of future networks, expedite the validation process, and reduce disputes regarding test results.

Benefits of Interoperability Testing Framework

Having a uniform set of tests[217, 218] levels the playing field for all potential network operators. An industry interoperability testing framework that has been developed by the industry as a whole and is readily available to all participants virtually eliminates any perception of unfair treatment in the validation process for safely interconnecting networks.

Alternative Approaches and Their Consequences

- Individual network operators using an informal set of tests . . . *puts the reliability of existing networks at greater risk due to non-comprehensive testing.*
- Ad hoc validation requirements . . . *results in unresolved disputes between new and existing network operators.*

[214] Key Finding 30, Interconnection testing is not based on a recognised standards-based framework section 3.3.
[215] Key Finding 61, Security integration and interoperability testing guidelines are inconsistent, Section 3.4.
[216] Key Finding 31, Interoperability testing between networks is often an overlooked function section 3.3.
[217] The ATIS PTSC-IOP Technical Report could be used as a starting point for the development of a European IP NNI Testing Framework.
[218] ETSI STF 328 (Specialist Task Force 328) for the development of interoperability test specs for IMS NNI has now been created by TISPAN WG6 (the TISPAN working group for testing).

- Mandated testing . . . *may result in unintended consequences such as tests that are not applicable in specific cases*.
- Testing not performed . . . *results in new networks connected based solely on an operator's request for interconnection and overall reliability and security are jeopardised.*

Next Steps

Suggested next steps to generate momentum toward the implementation of this Recommendation include:

8-1. The Private Sector creates a standardised network-to-network testing framework.

8-2. The Private Sector adopts the framework as the criteria for validation prior to connecting a new network to an existing network.

Measures of Success

The successful implementation of this Recommendation can be gauged by the following measures:

> **Agreements reached:** The network-to-network testing framework has been established by industry consensus and is readily available.
>
> **Testing occurs:** The network-to-network testing framework is actually being used to create specific test cases for interoperability confirmation.

4.9 Vigorous Ownership of Partnering Health

Background

Implementing each of the previous Recommendations will require cooperation within the industry and the development of a real partnership between industry and government. Interwoven throughout the discussions of the technical challenges facing Europe's future networks was serious concern about whether the necessary cooperation between the Private Sector and government could be achieved.[219, 220] *It is clear that it hasn't been achieved to this point.*[221, 222] *The Private Sector is somewhat fragmented, with new entrants seeking equal status with long established network operators. The industry is united however, in its desire for less regulation, while at the same time wanting to provide input to government decisions that affect the communications infrastructure and seeking access to sensitive information that might help them protect their infrastructure. Government stakeholders are reliant upon the expertise of service providers, network operators and equipment suppliers to make countless technology and operational decisions that will promote the public interest, but also have the responsibility to provide oversight regulation that they deem is in the public interest. A plethora of government-industry ICT cooperative initiatives demonstrates both sides' awareness of the need to work together,*[223] *however the symptoms observed throughout this Study's vast engagement with stakeholders lead to the diagnosis that too often, critical public-private partnerships are suffering from suboptimal health.*[224, 225, 226]

Recommendation 9
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.

Required Commitments

To sustain the viability of this Recommendation, the Private Sector, and Member State and European Institution governments must be committed to defined courses. Specifically,

(a) The Private Sector, Member States and European Institutions must recognise that the reliability, security and robustness of future networks is dependent upon the partnership which is developed between the various stakeholders.

(b) The Private Sector, Member States and European Institutions must recognise that the improvements to quality of life, and economic well-being that future networks offer will not be realised without ongoing cooperation between stakeholders.

[219] Key Finding 19, Emergency information sharing during incidents is limited, Section 3.2.
[220] Key Finding 40, Agreements, Standards, Policies and Regulations (ASPR) are Member State dependent, Section 3.3.
[221] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 15, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[222] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 16, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[223] A Google query with the search criteria [ICT Europe government industry partnership] returns over 1 million hits.
[224] Key Finding 21, Collaboration between governments and the Private Sector needs improvement, Section 3.2.
[225] Key Finding 23, Private sector disappointed in yield of government partnerships, Section 3.2.
[226] Key Finding 24, Government regulators are cautious regarding Private Sector claims, Section 3.2.

(c) The Private Sector, Member States and European Institutions must recognise that this partnership will not be successful without wholehearted commitment from each stakeholder.
(d) The Private Sector, Member States and European Institutions should set realistic expectations for the nature of public-private partnerships, given that ongoing tensions and rigorous debate on matters of interest and policy are expected and healthy.

Purpose

This Recommendation is aimed at *breaking through the impedance that too often stifles necessary collaboration of a critical public-private partnership, and thus wastes opportunities to collectively advance common interests regarding network availability and robustness*.

Benefits of Healthy Partnerships

The essential elements of healthy partnerships are *respect*, *commitment* and *integrity*. All three attributes are required of each party in dealing with its partners. Respect goes beyond fear or intimidation of the power held by the other party and should extend to genuinely valuing the legitimacy of the other's interests. Given the interdependence between government and the Private Sector, collaborating parties should respect the value that each side brings to the table.[227] *Commitment* requires each party embracing the stated objectives of the endeavour undertaken. This can take the form of sharing meaningful information or entering into frank discussions on hard issues. It is demonstrated by a willingness to work through obstacles and not give up in frustration, or worse, to participate passively as a disengaged party. *Integrity* is demonstrated by consistency between expressed positions and actions.

While the aim of both the Private Sector and the government is to provide reliable communications, they often find themselves in opposition because of sometimes competing interests. If respect, commitment and integrity are demonstrated consistently by collaboration leaders and participants, dialogue and progress can thrive. When conflict arises, it is critical for all parties involved to maintain their loyalty to the collaborative process and take on, if necessary, unilateral responsibility for its health, until the other parties are again properly engaged.

Alternative Approaches and Their Consequences

- Government and the Private Sector do not each take unilateral ownership of making the collaboration successful . . . *results in each side blaming the other for failures, the ultimate dissolution of meaningful partnership, and the weakening of Europe's future networks.*

Next Steps

The following steps are offered as suggestions to begin the process of implementing this Recommendation:

9-1. Private Sector companies should foster trust with government regulators by sharing accurate network availability and network robustness assessment results with appropriate government entities.[228]

[227] Key Finding 26, The Private Sector is not treated by government as an equal partner, Section 3.2.
[228] Key Finding 25, Companies are not committing expertise in engagements with government, Section 3.2.

9-2. Member States and European Institutions should engage industry representatives to collaborate on studies of identified issues at the *beginning* of a study.[229]

9-3. Member States and European Institutions should build trust with the Private Sector by providing them with leadership roles in appropriate studies on identified issues.

9-4. The Private Sector should share recommendations with appropriate government entities and incorporate government concerns where appropriate.

Measures of Success

The successful implementation of this Recommendation can be gauged by the following measures:

Industry Engaged: To what degree are Private Sector stakeholders included in government studies?

Government Engaged: To what extent does the Private Sector voluntarily share critical information with the government?

Collaboration Demonstrated: To what degree are these joint recommendations accepted and acted on?

[229] Key Finding 5, Government engages network operators too late, Section 3.1.

4.10 Discretionary European Expert Best Practices

Background

One of the milestones achieved during the ARECI Study was the confirmation by European experts of a core set of voluntary Best Practices that promote network reliability and security.[230] Best Practices are distinct from standards and regulations. They are another approach to influencing behaviour – by offering expert guidance to decision makers for implementation at their discretion.

Operating highly available, highly robust and highly secure communications networks depends heavily on expertise. The nature of this expertise involves several factors. First, these networks are extremely intricate. The reality of this irreducible complexity is a sea of never-ending cause–effect relationships and therefore a dependence on a very large number of experts with essential knowledge and familiarity. Secondly, these networks employ very sophisticated technologies that change rapidly. The consequence of this continuous inflow of innovation is again a dependence on a large number of experts with cutting edge skill and uncommon perspective. Finally, each network operator or service provider typically has some marked differences in its business approaches. The reality of this operational diversity is that outsider assumptions too often lack critical concrete insider insights. Given that most of Europe's ICT networks are owned and operated by the Private Sector, this is also where the critical mass of expertise resides. Industry consensus Best Practices are the most effective way to capture expertise and make it available to the broader industry.

Recommendation 10

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.

Required Commitments

To sustain the viability of this Recommendation, the Private Sector, Member States and European Institutions must be committed to defined courses. Specifically,

(a) The Private Sector must initiate collaboration to share expertise, develop consensus on Best Practice guidance, and maintain the collection of this guidance.

(b) Service providers, network operators and equipment suppliers must take seriously their responsibility regarding the discretionary implementation of Best Practices.[231]

(c) Government powers must respect the Private Sector Best Practice development process as not intended to be one in which ideas and principles shared can be used against those contributing them. Government powers must therefore abstain from using Best Practices collaboration efforts as a step toward regulation.[232]

[230] Key Finding 52, European communications industry experts confirmed core set of Best Practices, Section 3.3.
[231] Key Finding 53, Private sector implementation of European-confirmed Best Practices is high, Section 3.3.
[232] Key Finding 32, Both incumbents and new entrants consider regulation undesirable, Section 3.3.

(d) The Private Sector, Member States and European Institutions must work together as equal, trusted partners to ensure the proper focus and level of effort for these initiatives.

Purpose

This Recommendation addresses the issue of *how to ensure that the best expertise is engaged in promoting the availability and robustness* of Europe's electronic communications infrastructures.

Role of Best Practices

Appreciation for the value of voluntarily-implemented, industry-consensus Best Practices comes from understanding both the nature and vital role of expertise in this sector. This Recommendation *aligns* technical policy development with its essential dependence on expertise in the Private Sector. More information on the unique and vital role of Best Practices is provided in Section 2.5.3.

Alternative Approaches and Their Consequences

- Government mandates on aspects of network design or operation . . . *may result in unintended consequences by failing to appreciate and anticipate this sector's complexity, evolving technology, and diversity of business approaches.*
- Government gives an appearance of engaging its expertise, but ultimately values it as secondary to other concerns . . . *government misses an opportunity to further optimise network availability and robustness.*
- The Private Sector fails to demonstrate its commitment to ensure needed levels of network availability and robustness . . . *forcing government to fulfil their oversight obligations through regulation.*
- Continue on the current course where European Institutions and Member States too often involve the Private Sector in a minimal way, and the Private Sector is not regularly engaged in collaborative efforts to share its collective expertise[233] . . . *will likely result in suboptimal network availability and robustness and an inability to quickly respond to future catastrophes.*

Next Steps

10-1. Service Providers, Network Operators, and Equipment Suppliers should willingly implement the Best Practices, confirmed by European experts during the ARECI Study, where appropriate. Each of the 71 Best Practices, found on following web site (www.bell-labs.com/EUROPE/bestpractices/) are considered as effective or moderately effective by 90% of the European subject matter experts involved.[234]

10-2. Service Providers, Network Operators and Equipment Suppliers should build on the Best Practices already established by participating in similar efforts.

10-3. European Institutions and Member State governments should encourage the Private Sector's initiative to formulate Best Practices and their voluntary implementation by publicly articulating its preference for more expert-based guidance and its appreciation for the Private Sectors' initiatives in these areas.

[233] Key Finding 5, Government engages network operators too late, Section 3.1.

[234] ~100 European subject matter experts provided input on the effectiveness of these Best Practices; includes virtual survey and experts workshop participants.

Measures of Success

The successful implementation of this Recommendation can be gauged by the following measures:

Expertise Engaged: To what degree are Private Sector stakeholders sending their subject matter experts to industry Best Practice collaboration efforts?[235]

Best Practices Implemented: Are service providers, network operators and equipment suppliers, implementing Best Practices, where appropriate?

Trust Fostered: Are European Institution and Member State regulatory measures restrained in areas where the Private Sector is taking the necessary initiative?

[235] An example of this commitment was demonstrated in the four European Experts Workshops held during October and November, 2006 with joint technical sponsorship by the IEEE CQR and Bell Labs. Proceedings of the Experts Workshops are published on www.comsoc.org/~cqr/EU-Proceedings-2006.html The workshops were held in Rome, London, Berlin and Brussels and hosted by the Italian Ministry of Communications, BT, Rohde & Schwarz SIT, and SWIFT, respectively.

This page is intentionally left blank

5 CONCLUSION

Europe's future communications networks promise to usher in a new world of business and lifestyle-enhancing capabilities – many of which have not yet even been imagined. Relatively recent advances of ICT in the areas of affordable pricing, mobility, geo-locating, video imaging and search engines – while breathtaking – are likely only the beginning of an ever-accelerating pace of the same for the foreseeable future.

This Study submits ten major Recommendations to European Institutions, Member States, and the Private Sector *for the express purpose of promoting the availability and robustness of Europe's communications networks*. Each major Recommendation is accompanied by an explanation of measures of success, next steps, and alternatives and associated consequences. These extraordinary elements are added to these Recommendations because of the *criticality* and *urgency* regarding their implementation.

The *critical* priority for implementation is quite explicit for this subject. Without communications networks and services, public welfare is endangered, economic stability is susceptible, other critical sectors are exposed, and countless other direct and indirect misfortunes will avoidably occur. Incredible benefits are being enjoyed as society increasingly relies on sophisticated technologies. The price for these benefits is living with the dependency on these networks. The *urgency* for implementation is *not* something of Europe's choosing. The utter dependency on these networks demands it. Europe can *not* afford to:

1. *Be unprepared for disasters*
2. *Have the most mission critical communications in a crisis blocked*
3. *Not harness the full capability of industry to deal with emergency situations*
4. *Incur network impairment because information was not shared*
5. *Experience an infrastructure collapse from a cross-sector failure*
6. *Lose control of network systems or traffic*
7. *Have network standards not tuned to unique European needs*
8. *Allow "weakest link" networks to compromise the interconnected networks*
9. *Be guided by suboptimal policies due to stifled collaboration*
10. *Leave the power of its collective expertise estranged and unengaged*

Each of these failures can be avoided by the Recommendation corresponding to its number. The implementation of this report's Recommendations will mean great strides in reducing each of these and other risks.

While the urgency is pressing, the long term benefits of reliable communications networks are incomparable. The people of Europe stand to benefit immeasurably from the anticipated protection of life, economic efficiency, citizen connectivity, functional flexibility, and speed. **This Study strongly urges European Institutions, Member States and Private Sector stakeholders to chart, and embark on, a new course of policy and practice that forcefully advocates highly available and highly robust communications infrastructure.**

This page is intentionally left blank

ACKNOWLEDGEMENTS

The following organisations and individuals are acknowledged for their role in the successful completion of this Study, the formulation of its guidance, and ultimately the improvements in network availability and robustness that are eagerly anticipated.

First and foremost, the Study team recognises the **many subject matter experts** of the communications industry and the public servants who are passionate about improving the network reliability and network security of Europe's communications infrastructure. This Study could not have been completed without their insights, energy and commitment. The Study team also recognises their organisations for their needed support.

The Study team also expresses special appreciation to the four stakeholders who served their European communities by hosting the strategic experts workshops:

- **Dr. Luisa Franchina,** *Director General - **Italian Ministry of Communications***
  - Workshop 1: Rome Italy
- **David Donegan,** *Head of Business Continuity - **BT Group***
  - Workshop 2: London, United Kingdom
- **Harry Kaube,** *Head of Sales, Germany- **Rohde & Schwarz SIT***
  - Workshop 3: Berlin, Germany
- **Didier Verstichel,** *Director, Enterprise Security & Architecture - **SWIFT***
  - Workshop: Brussels, Belgium

Each workshop facility received a 100% satisfaction rating from the participants.[236]

Special appreciation is also expressed to the **IEEE Communications Society Technical Committee on Communications Quality & Reliability (CQR)** for leadership in joining Bell Labs as joint technical sponsor for the four experts workshops: in particular, expert workshop co-chairs **Peter Hoath** (BT) and **Rick Krock** (Bell Labs, Alcatel-Lucent) and CQR Chair **Dr. Kenichi Mase** (Niigata University) and CQR Chair-Elect **Dr Chi-Ming Chen** (AT&T).

Finally, the Study team acknowledges the **staff of the European Commission** for the value they provided through their oversight for the ARECI Study project. Specifically, the Study team appreciated the staff's review of interim reports, their assistance in various aspects of outreach, and their organization of the ARECI Public Forum in Brussels.

[236] www.comsoc.org/~cqr/EU-Proceedings-2006.

This page is intentionally left blank

ARECI STUDY TEAM

The qualifications for team members were very high. Each selected team member has industry recognised expertise in the subject matter areas they supported. Given the importance of the mission, individuals considered serving on the ARECI Study Team as a distinct honour. The structure of the ARECI Study team experts had several components:

- Leaders
- Core Study team
- Executive Support
- Key Contributors and Key Supporters

	Power	Environment	Software	Hardware	Payload	Networks	Human	Policy
Leaderhip								
Mario Corrado								■
Karl Rauscher	■	■	■	■		■	■	■
Aleksei Resetko			■			■		
Core Team								
Stu Goldman			■		■	■		■
Rick Krock	■	■		■		■	■	■
Steve Richman	■				■	■		
Jim Runyon	■		■	■		■		■
Himanshu Pant						■		
Supporting Members								
Ray Bonelli			■	■			■	■
Peter Hayden	■							
Guido Nienkemper		■				■	■	
Suhasani Sabnis						■		
Rao Vasireddy						■		

Figure 17: Distribution of Team Expertise

Leaders

QUINTO MARIO CORRADO served in the important role of managing the ARECI Study interface with the EC customer. In this capacity, he provided guidance and counsel to the team regarding expectations for contract fulfilment, related EU initiatives, and general guidance on the EC operation and management.

Quinto Mario Corrado began his carrier in Brussels with an internship at the European Commission in 1991. Since then, he has been subsequently working for consultancy firms in Brussels in, among others, a number of projects co-financed with the EC support (like Euromanagement and the Community Initiative Integra), and working as a consultant for studies and publications tendered by the EC (i.e. Inforegio and European Social Fund report). Quinto Mario has also published with a major Italian publishing house (Sperling & Kupfer) a survey on the EC policies in economic development field. Quinto Mario joined Lucent in 2000, with responsibilities for the services business in Southern Europe and has been covering various positions since then. He is presently the Alcatel-Lucent Services Sales manager for Belgium and Luxembourg.

KARL RAUSCHER served as the Bell Labs leader of the ARECI Study and architect of the Study's methodology, providing vision and guidance for the core team. He set the direction by ensuring the use of the eight ingredient framework and by advancing the concepts of an industry ‘experts workshops,’ and the virtual interviews. In addition, Karl modeled consensus building leadership at the experts workshops and lent his vast government-industry technical policy expertise to the discussion, and to the writing of the final report. He is the chief author of Recommendations 9 (Vigorous Ownership of Partnering Health) and 10 (Discretionary European Best Practices).

Karl Rauscher is a Bell Labs Fellow cited for the first achievement of 6 ‘9’s reliability performance for a public network switching system, being instrumental in shaping the post September 11, 2001 U.S. homeland security strategy and being at the forefront in the development of hundreds of industry expert Best Practices. He is the executive director of the Bell Labs Network Reliability and Security Office, and has provided leadership for numerous critical government-industry fora, including serving as the Network Reliability Steering Committee (NRSC) vice chair, FCC Network Reliability and Interoperability Council (NRIC) Best Practices focus group (wireless networks, data networks, homeland security) chair, and the President’s National Security Telecommunications Advisory Committee (NSTAC) Industry Executive Subcommittee (IES) vice chair, IEEE CQR advisory board chair, IEEE Communication Society Strategic Planning Committee member. He has been an advisor for network reliability issues on five continents and has served as an expert witness for the U.S. Congress Select Committee on Homeland Security regarding the Power Blackout of 2004. He is also the founder and president of the non-profit Wireless Emergency Response Team (WERT) that conducts search and rescue efforts using advanced wireless technology. He is the recipient of numerous industry awards and honors for service in crises and for industry leadership. He holds a Bachelor of Science degree with high distinction in electrical engineering from Penn State University in University Park, Pennsylvania, a Masters degree in electrical engineering from Rutgers University in New Brunswick, New Jersey, and a Masters degree with high honors in Biblical Studies from the Dallas Theological Seminary in Texas. He has over 20 years of experience in the communications industry.

ALEKSEI RESETKO served as the ARECI Study project manager, having overall responsibility of the Study execution and quality of deliverables. In addition, he chaired the third experts workshop on hardware and software, and performed numerous interviews with key European Stakeholders.

Aleksei Resetko is senior security and reliability expert in European Alcatel-Lucent Security Practice, and has over 8 years of professional experience in the area of Security, Reliability and ICT Risk Management. His core competencies are reliability and security of complex networks, auditing of ICT management procedures and security program development. His experience spans sectors that include communication service providers, finance, transportation, education and the public sector. He is a frequent speaker at ICT security and reliability related conferences and has numerous professional publications. He holds a Master of Science in economics (University of Heidelberg), Certified Information Systems Auditor (CISA) and Certified Information Systems Security Professional (CISSP).

Core Team

The core team developed the ARECI Study, led the experts workshops, identified Key Findings, developed Recommendations and co-authored the ARECI final report.

STUART O. GOLDMAN co-hosted the second experts workshop on networks and payload held in London, UK. He is a subject matter expert for the payload, network and policy/ASPR ingredients. He is also chief author of Recommendations 2 (Priority Communications on Public Networks), 7 (Unified European Voice in Standards) and 8 (Interoperability Testing).

Stuart O. Goldman is a consulting member of technical staff in the standards department for Alcatel-Lucent in Phoenix, Arizona. Stuart has developed system requirements for switching and cellular products. His recent efforts have focused on Public Emergency Calling (9-1-1), and government authorised Emergency Telecommunications Services. He holds 17 patents. He is an acknowledged leader in the international standards industry. He is the chair for ATIS Packet Technologies and Systems Committee (PTSC) Interoperability (IOP) subcommittee, the past co-chair for the ATIS Network Interoperability Forum (NIIF), and the vice chair for the ATIS PTSC Signaling, Architecture, and Control (SAC) subcommittee. He has 35 years of telecommunication development experience and holds a B.S. degree in Physics from Roosevelt University.

RICHARD E. KROCK hosted the first experts workshop on power and environment held in Rome, Italy. He is a subject matter expert in the power, environment, network and policy/ASPR ingredients. He is also the chief author of Recommendations 1 (Emergency Preparedness), 3 (Mutual Aid) and 4 (Critical Infrastructure Information Sharing). He also served as an editor for several sections of the final report.

Richard E. Krock is a member of technical staff in the Services Technology department at Alcatel-Lucent Professional Services in Lisle, Illinois, and has served as a member of the Bell Labs Network Reliability and Security Office for five years. His responsibilities include the analysis of network outages and the identification and implementation of countermeasures. He has been an active member of the past two FCC Network Reliability and Interpretability Councils and has led various sub-teams related to power. He has provided consulting services on emergency preparedness/disaster recovery both domestically and internationally, and also represents Alcatel-Lucent at the Telecom Information Sharing and Analysis Center, part of the National Coordinating Center for Telecommunications. Mr. Krock holds a B.S. degree in electrical engineering from Valparaiso University in Indiana and an M.B.A in telecommunications from Illinois Institute of Technology in Chicago. He is also a licensed professional engineer.

HIMANSHU PANT provided coordination for the initial phase of stakeholder interviews and had primary responsibility for developing the Technical Descriptions (Annex E) that reviews a wide range of future networks. Himanshu is a subject matter expert in the networks ingredient.

Dr. Himanshu Pant is a distinguished member of technical staff in the High Availability and Security Networks group at Bell Labs. Himanshu has over 15 years of experience in the telecommunications industry concentrating in the areas of system

and network quality, reliability and security. Himanshu holds the M.S and Ph.D. degrees in Mathematics from Northwestern University in Evanston, Illinois. He has published in refereed journals such as IEEE Transactions on Reliability and Bell Labs Technical Journal and presented papers at a number of communications industry conferences. Himanshu, a Senior Member of the IEEE, Chairs the Aerospace and Electronic System/Engineering Management Chapter of the New Jersey Coast Section of IEEE and is a Certified Information Systems Security Professional (CISSP).

STEVEN H. RICHMAN prepared the proposal that led to the AREI Study contract award and led the initial phase and deliverables of the Study. He is a subject matter expert in the networks ingredient. He also provided oversight of the Technical Description (Annex E) of the final report. He is the chief author of Recommendation 5 (Inter-Infrastructure Dependency).

Dr. Steven Richman is the director of the High Availability and Security Networks organisation in Alcatel-Lucent, Bell Labs. He has been a systems engineer in the field of data communications networking for almost 40 years and has concentrated on the application and introduction of new communications technology and services with appropriate network integrity. His experience in data communications and Internet systems covers service realisation and deployment, network planning and design, service continuity and recovery, confidential communications and standardisation of performance and security in the U.S. and national standards organisations. He is currently responsible for planning, assessing and recommending solutions for next generation network and service reliability, the interdependence of the U.S. critical infrastructure on telecommunications. He is certified as an Information Systems Security Professional (CISSP). He earned his PhD EE and MSEE degrees from the Polytechnic Institute of Brooklyn in 1971 and 1968, respectively, and his BSEE degree from the City College of New York in 1967. He is a senior member of the IEEE and a member of the Eta Kappa Nu, Tau Beta Pi and Sigma Xi honor societies.

JAMES P. RUNYON hosted the second experts workshop on networks and payload in London, UK. He is the chief author of Recommendation 6 (Supply Chain Integrity and Trusted Operation). He is a subject matter expert for network, software and hardware ingredients. He was the managing author and editor for the final report.

James P. Runyon is a technical manager in the Network Reliability Office at Bell Labs in Naperville, Illinois. He holds a B.S. degree in chemistry from Taylor University in Upland, Indiana and an M.S. degree in computer science from the University of Wisconsin in Milwaukee. Prior to becoming technical manager, he was a distinguished member of technical staff in software feature development, systems engineering and network architecture for communications systems, and for 10 years he served as an architecture manager for Lucent's ADSL, cable TV and fiber-to-the-home broadband platforms. He has been awarded four U.S. patents and has multiple publications in the Bell Labs Technical Journal and other industry forums. In the last few years, Mr. Runyon has been an active participant in a number of FCC-charted federal advisory committees. As a member of the Network Reliability Steering Committee (NRSC), he *has provided leadership in five significant studies on network outages. Mr. Runyon is a member of IEEE, a member and administrator for several FCC Network Reliability and Interoperability Council (NRIC) focus groups, and serves as manager for the public and internationally-renown Best Practice web site.*

Key Contributors and Supporters

Other individuals made key contributions to the ARECI Study and final report. Their contributions included providing team training, establishing interview criteria, conducting interviews, reviewing document content and Recommendations, and providing guidance and support throughout the project. Others listed here provided supplemental support to the technical aspects, such as executive guidance and customer team logistics.

Executive Support

- Luis Eguiagaray - project director, steering committee
- Guido Nienkemper - project management oversight, steering committee, customer satisfaction management, ongoing team support, quality control and deliverable assurance
- Carlos Solari - network security and Recommendation 6
- Rati Thanawala - steering committee, proposal advocacy

Other Contributors and Supporters

- Gianluca Anconitano - Internet technical descriptions, Rome workshop
- Azfar Aslam - cable and Internet market trends
- Krystian Baniak - WiFi and WiMax technical descriptions
- Fred Battaglia - WiFi market trends
- Peter Benedict - public relations
- Ray Bonelli - ARECI core team trainer, industry-government collaboration
- Mark Burnworth - public relations
- Jayant Deshpande - IP network technical descriptions
- Christine Diamente - EC government affairs
- Deirdre Doherty - PSTN/IN technical descriptions
- Alan Dye - London workshop support
- Martin Glapa - cable technical descriptions
- Christian Grégoire - execution of ARECI Public Forum
- Emma Griffiths - London workshop support
- Peter Hayden - power ingredient
- Michael Huffaker - technical descriptions
- Paul J. Justl - PSTN and WiMax market trends
- Anil Macwan - human-machine interfaces, human performance
- Bernie Malone III - emergency communications
- Richard Morrell - cable technical descriptions
- Amit Mukhopadhyay - 3G network technical descriptions
- Samphel Norden - 3G network and Wireline and 3G VoIP security
- Guru B. Patil - multiple technology market trends
- Michela Petri - Rome workshop
- Devon Prutzma - web site development
- Marco Raposo Melo - support during interview phase of the Study
- Suhasani Sabnis - network security
- David Shaw - London workshop support
- Gina Shih - 3G WCDMA market trends

- Rao Vasireddy - network security
- Ward Vrijsen - Internet technical descriptions
- Robert Waldstein - web development

EURESCOM was a research partner in conducting this Study; the following individuals were contributors to this Study:

- Adam Kapovits
- Anastasius Gavras
- Halid Hrasnica
- Milon Gupta

GLOSSARY

Availability
Availability is simply the extent to which a system is ready to be called into use for its designated purpose, without advance knowledge of when it is needed. In this Study, the system is Europe's electronic communications infrastructures, which are made up of many networks. A more formal definition of availability is offered as follows:

> The degree to which a system, subsystem, or equipment is operable and in a committable state at the start of a mission, when the mission is called for at an unknown, i.e., a random, time.[237]

Network or service availability characterises the network or service being operable for use, as intended, at any given instant. It is a function of the underlying system(s) reliability, robustness of technology and design and reparability or restorability. Network design includes appropriate redundancy, alternate routes and sufficient or additional capacity. Availability is expressed in multiple ways, such as, the duration of time, the probability, and the percent of time, that the network is operable. Conversely, the time per interval during which the network is inoperable (i.e., unavailability) sometimes is the indirect measure of availability. The duration of (operable or inoperable) time may be continuous or non-continuous.

$$TotalTimeAvailable = T_A = \sum_i T_{Operable(i)}$$

$$TotalTimeUnavailable = T_U = \sum_j T_{Inoperable(j)}$$

$$Availability = \frac{T_A}{(T_A + T_U)}$$

$$Unavailability = T_U$$

where

$$T_A + T_U = TotalTimeInterval = T_I$$

For example, current system platforms are commonly described as highly available if they are operable at least "five-nines" (e.g., 99.999% or better). This corresponds to less than five minutes of cumulative inoperable or downtime, per year.

Critical Communications Infrastructure
Some Best Practices are intended for critical communications infrastructure. Because of the complex, sensitive and proprietary nature of this subject, critical communications infrastructure is defined by its owners and operators. Generally, such distinction applies to points of concentration, facilities supporting high traffic, and network control and operations centers, and equipment supplier technical support centres.

New Entrant
New entrants typically base their business offering new technologies such as IP-based routing, etc. New entrants may also include new divisions within incumbent companies that are established to compete with, or offer similar services, as new companies.

Outage
A condition in which a user is completely deprived of service by the system. *Note:* For a particular system or a given situation, an outage may be a service condition that is below a defined system operational threshold, *i.e.,* below a threshold of acceptable performance.[238]

[237] ATIS Telecom Dictionary. www.atis.org
[238] ATIS Telecom Glossary 2000, T1.523-2001, www.atis.org/tg2k/

Reliability

Reliability is simply the likelihood that a system will perform its intended function within the context it was designed to operate within.[239]

A measure that refers to a particular "mission". It represents the ability of the system, subsystem, equipment, network, or service to operate for the intended purpose, during the intended period of time. It is the probability that given operability now, it sustains operation for a period of time. For example, the reliability of the space shuttle, would refer to it's operability during the period of time which includes its launch, time in space and return to Earth. Thus, reliability is often characterised as a probability or per cent or may also be characterised as the Mean Time Between Failure (MTBF).

The ability to achieve high availability is also a factor of how quickly a system, subsystem, equipment, network, or service can be repaired or service restored when a failure occurs. Reparability or Restorability are respectively characterised by the Mean Time To Repair or Mean Time To Restore (MTTR). First an foremost is the return to operability of the intended function. This may occur through an equipment repair, or more likely an equipment substitution, redundancy or alternate means for the intended use. Hence, in telecom, Mean Time to Restore (service) is most often the key measure.

Robustness

The ability to withstand and recover from adverse effects on the system, subsystem, equipment, network, or service. Adverse effects may manifest themselves directly as unavailability, or indirectly as performance (delay, throughput, packet loss, session stability) degradations and the effects of security threats on inherent security vulnerabilities. The ability of the technology, design or systems themselves to adjust capacity, reroute traffic, reconfigure, discard malicious packets and failover, for example, affects robustness to these situations.

Sector

A group of industries of infrastructures that perform a similar function. In general, critical sectors are sectors whose incapacitation or destruction would have a debilitating impact on the national security and the economic and social well-being of a nation.[240]

Threat

A threat is an attempt to exploit one or more vulnerabilities that may result in damage to or compromise of a system (e.g., ICT network) or some portion of it.[241]

Vulnerability

A vulnerability is an intrinsic characteristic of an infrastructure or system (e.g., ICT network or network components) that make it susceptible to damage or compromise if exploited by a threat.

[239] A more formal definition from the ATIS Telecom Glossary. **reliability:** 1. The ability of an item to perform a required function under stated conditions for a specified period of time. 2. The probability that a functional unit will perform its required function for a specified interval under stated conditions. 3. The continuous availability of communication services to the general public, and emergency response activities in particular, during normal operating conditions and under emergency circumstances with minimal disruption.

[240] International Critical Information Infrastructure Protection (CIIP) Handbook 2004, , An Inventory and Analysis of Protection Policies in Fourteen Countries, Swiss Federal Institute of Technology, p. 227.

[241]Network Reliability and Interoperability Council VI, Homeland Security – Physical Security (Focus Group 1A) – Prevention Report, Issue 1, Dec. 2002, p. 27, www.nric.org/fg/nricvifg.html;
Network Reliability and Interoperability Council VI, Homeland Security – Physical Security (Focus Group 1A) – Prevention and Restoration Report, Issue 2, Mar. 2003, pp.27, 41, www.nric.org/fg/nricvifg.html;
Network Reliability and Interoperability Council VI, Homeland Security – Physical Security (Focus Group 1A) – Final Report, Issue 3, Dec. 2003, www.nric.org/fg/nricvifg.html;
Network Reliability and Interoperability Council VII, Focus Group 3A – Wireless Network Reliability – Final Report, Issue 3, Sept. 2005, www.nric.org/fg/index.html;
Network Reliability and Interoperability Council VII, Focus Group 3B – Public Data Network Reliability – Final Report, Issue 3, Sept. 2005, www.nric.org/fg/index

ACRONYMS

3G	Third Generation Wireless
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorisation and Accounting
ACL	Access Control List
ADSL	Asymmetrical Digital Subscriber Line
AES	Advanced Encryption Standard
AGCF	Access Gateway Control Function
AMG	Access Media Gateway
AMPU	Average EBITDA margin per user
AMS-IX	Amsterdam Internet Exchange
AP	Access Point
ARECI	Availability and Robustness of Electronic Communications Infrastructures
ARPU	Average Revenue Per User
ASP	Application Service Provider
ASPR	Agreements, standards, policy and regulation
AS	Autonomous System
ATIS	Alliance for Telecommunications Industry Solutions
ATIS PRQC	Network Performance, Reliability, and Quality of Service Committee
ATM	Asynchronous Transfer Mode
AuC	Authentication Center
BDSL	Broadband Digital Subscriber Line
BG	Border Gateway
BGCF	Breakout Gateway Control Function
BGP	Border Gateway Protocol
BH	Busy Hour
BICC	Bearer Independent Call Control
BP	Best Practice
BRI	Basic Rate Interface
BSC	Base Station Controller
BSS	Business Support System
BSSAP	Base Station Subsystem Application Part
BWA	Broadband Wireless Access
C7	CCITT Signalling System #7
CAC	Call Admission Control
CAGR	Compound Annual Growth Rate
CAMEL	Customized Application of Mobile network Enhanced Logic
CDMA	Code Division Multiple Access
CE	Customer Edge (router)
CENELEC	European Committee for Electro-technical Standards
CEPT	European Conference of Postal & Telecommunications Administrations
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIDR	Classless Inter-Domain Routing
CM	Cable Modem
CMTS	Cable Modem Temination System
CO	Central Office
COTS	Commercial Off The Shelf
CPE	Customer Premises Equipment
CQR	Communications Quality and Reliability
CS	Circuit Switched
CSCF	Call Session Control Function
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DAIDALOS	An EU IST Research Project
DiffServ	Differentiated Services

DLC	Digital Loop Carrier
DNS	Domain Name Server
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DOCSIS	Data over Cable System Interface Specification
DOS	Denial Of Service
DSCP	Differentiated Service Code Point
DSSS	Direct Sequence Spread Spectrum
DSL	Digital Subscriber Line
DLSAM	DSL Access Multiplexer
DWDM	Dense Wavelength Division Multiplexing
EAP	Extensible Authentication Protocol
EBITDA	Earnings Before Interest, Taxes, Depreciation and Amortisation
EDGE	Enhanced Data-rate for GPRS Evolution
EICTA	European Information & Communications Technology Industry Association
EIR	Equipment Identity Register
EMITA	Embedded Multimedia Terminal Adapter
EMC	Electro-Magnetic Compatibility
ENISA	European Network and Information Security Agency
ES	Equipment Supplier
ETP	European Telecommunications Platform
ETS	Emergency Telecommunications Service
ETSI	European Telecommunication Standards Organisation
EU	European Union
EVDO	Evolved Data Only – a 3G mobile standard
FACA	Federal Advisory Committee Act
FCC	Federal communications Commission
FGNGNFRA	Focus Group on NGN Functional Requirements and Architecture
FHSS	Frequency Hopping Spread Spectrum
FQDN	Fully Qualified Domain Name
FR	Frame Relay
GGSN	Gateway GPRS Support Node
GIS	Geographical Information Systems
GMSC	Gateway Mobile Services Switching Centre
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HFC	Hybrid Fibre Coax
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IAD	Integrated Access Device
IANA	Internet Assigned Numbers Authority
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IMS	IP Multimedia Subsystem – a 3G mobile network standard
IN	Intelligent Network
INAP	Intelligent Network Application Part
IntServ	Integrated Services
IOP	Interoperability
IP	Internet Protocol
IPRAN	IP Radio Access Network
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
IPTV	Internet Protocol Television

IRTF	Internet Research Task Force
IS-IS	Intermediate System to Intermediate System
ISDN	Integrated Services Digital Network
ISO	International Standards Organisation
ISOC	Internet Society
ISP	Internet Service Provider
ISUP	ISDN User Part
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union -Telephony sector
LAN	Local Area Network
LINX	London Internet Exchange
LMR	Land Mobile Radio
LSP	Label Switched Path
LSR	Label Switching Routers
M&P	Methods and Procedures
MAN	Metro Access Network
MANETS	Mobile Ad hoc Networks
MAP	Mobile Application Part
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
MRCN	Mobile Radio Controlled Network
MPLS	Multi Protocol Label Switching
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MRS	Media Resource Server
MSC	Mobile service Switching Centre
MSISDN	Mobile Subscriber Integrated Services Digital Network
MTBF	Mean Time Between Failures
MTP	Message Transfer Part
MTTR	Mean Time To Repair
MUSE	An EU IST Research Project
NAT	Network Address Translation
NCC	Network Coordination Centre
NG-DSLAM	Next Generation Digital Subscriber Loop Access Multiplexer
NGN	Next Generation Networks
NLOS	Non-Line-Of-Sight
NO	Network Operator
NOBEL	An EU IST Research Project
NRIC	Network Reliability & Interoperability Council
NRSC	Network Reliability Steering Committee
NSCC	National Infrastructure Coordination Centre
NSTAC	National Security Telecommunications Advisory Committee
OAM	Operations Administrations and Management
OAM&P	Operations, Administration, Maintenance & Provisioning
OBAN	An EU IST Research Project
OMA	Open Mobile Alliance
OSA	Open Service Architecture
OSI	Open System Interconnection
OSPF	Open Shortest Path First
OSS	Operations Support System
P2P	Peer to Peer
PDA	Personal Digital Assistant
PDF	Policy Decision Function
PD-FE	Policy Decision - Functional Entity
PDSN	Packet Data Service Node
PE	Provider Edge (router)
PHB	Per Hop Behaviour
PLMN	Public Land Mobile Networks

PoE	Power over Ethernet
POP	Point of Presence
POS	Packet Over Sonet
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PS	Packet Switched
PSTN	Public Switched Telephone Network
PToC	Push to Talk over Cellular
PTSC	Packet Technologies and Systems Committee
PVC	Permanent Virtual Circuits
QoS	Quality of Service
RACF	Resource and Admission Control Functions
RBAC	Role Based Access Control
RFC	Request for Comments
RIP	Routing Information Protocol
RIPE	Reseaux IP Europeens
RNC	Radio Network Controller
RoI	Return on Investment
SAC	Signalling, Architecture, and Control
SBC	Session Border Controller
SCCP	Signalling Connection Control Part
SCP	Switching Control Point
SDH	Synchronous Digital Hierarchy
SG	Signalling Gateway
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMF	Single Mode Fibre
SMS	Short Messaging Service
SMSC	SMS Inter-Working MSC
SP	Service Provider
SS7	Signalling System #7 (C7)
SSF	Service Switching Function
SLA	Service Level Agreement
SME	Subject Matter Expert
SONET	Synchronized Optical Networking
SP	Service Provider
STB	Set Top Box
STP	Spanning Tree Protocol
TCAP	Transaction Capabilities Application Part
TCO	Total Cost of Ownership
TDD	Time Division Duplex
TDM	Time Division Multiplex
TE	Traffic Engineering (as in RSVP-TE)
TFTP	Trivial File Transfer Protocol
TETRA	Terrestrial Trunked Radio
TIA	Telecommunications Industry Association
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TKIP	Temporary Key Integrity Protocol
TLS	Transport Layer Security
TOS	Type of Service
TRC-FE	Transport Resource Control - Functional Entity
TOS	Type Of Service
UMTS	Universal Mobile Telecommunication Service
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier
UTRAN	UMTS Terrestrial Radio Access Network

VLAN	Virtual LAN
VLR	Visitor Location Register
VOD	Video on Demand
VoIP	Voice over IP
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
W3C	World Wide Web Consortium
WAN	Wide Area Network
WARP	Warning, Advice and Reporting
WCDMA	Wideband Code Division Multiple Access
WiFi	Wireless Fidelity
WiMAX	World Interoperability for Microwave Access
WTSA	World Telecommunications Standards Organisation
Y2K	Year 2000
VoIP	Voice over IP

This page is intentionally left blank

BIBLIOGRAPHY

[1] 3G Wireless Broadband, *“Informa telecoms and media,”* Volume 8, Issue 12, July 2006.

[2] 3GPP, *“3rd Generation Partnership Project: Technical Specification Group Services and Systems Aspects; Network architecture (Release 1999),”* TS 23.002 V3.6.0 (2002-09) (www.arib.or.jp/IMT-2000/V600Dec06/5_Appendix/R99/23/23002-360.pdf); © 2002, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC), All rights reserved, 650 Route des Lucioles - Sophia Antipolis, Valbonne – France.

[3] 3GPP, *“3rd Generation Partnership Project: Technical Specification Group Services and Systems Aspects; Network architecture (Release 4),”* TS 23.002 V4.8.0 (2003-06), www.arib.or.jp/IMT-2000/V460Nov05/5_Appendix/Rel4/23/23002-480.pdf; © 2002, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC), All rights reserved, 650 Route des Lucioles - Sophia Antipolis, Valbonne – France.

[4] 3GPP, *“3rd Generation Partnership Project: Technical Specification Group Services and Systems Aspects; Network architecture (Release 5),”* TS 23.002 V5.12.0 (2003-09), www.arib.or.jp/IMT-2000/V480May06/5_Appendix/Rel5/23/23002-5c0.pdf; © 2002, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC), All rights reserved, 650 Route des Lucioles - Sophia Antipolis, Valbonne - France.

[5] 3GPP, *“3rd Generation Partnership Project: Technical Specification Group Services and Systems Aspects; Network architecture (Release 6),”* TS 23.002 V6.10.0 (2005-12), www.arib.or.jp/IMT-2000/V600Dec06/5_Appendix/Rel6/23/23002-6a0.pdf; © 2002, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC), All rights reserved, 650 Route des Lucioles - Sophia Antipolis, Valbonne - France.

[6] Alliance for Telecommunications Industry Solution (ATIS), *“ATIS Telecom Glossary 2000,”* T1.523-2001, www.atis.org/tg2k/.

[7] Alliance for Telecommunications Industry Solution (ATIS) Network Reliability Steering Committee (NRSC), *“2002 Annual Report,”* www.atis.org/nrsc.

[8] Alliance for Telecommunications Industry Solution (ATIS) Network Reliability Steering Committee (NRSC), *"Procedural Outage Reduction; Addressing the Human Part,”* NRSC Report May 13, 1999.

[9] Alliance for Telecommunications Industry Solution (ATIS) Performance, Reliability, and Quality of Service Committee (PRQC), *“PRSSC – T1A1.2/2003-148, Appendix B,”* www.atis.org/0010/index.asp.

[10] Walt Beyeler, Stephen Conrad, Thomas Corbet, Gerard P. O'Reilly, David D. Picklesimer, *"Inter- Infrastructure Modelling - Ports and Telecommunications,"* Bell Labs Technical Journal, Volume 9, Number 2, 2004, 91-105.

[11] Bitpipe, www.bitpipe.com/tlist/Telecommunications-Infrastructure.html.

[12] U. Black, *“ATM Foundation for Broadband Networks,”* Volume I, 2nd Edition., Prentice Hall, Upper Saddle River, NJ, 1999.

[13] British Broadcasting News – International Version, *“Bid to Overhaul Europe Power Grid,” news.bbcc.co.uk/2/hi/europe/6117880.stm?ls*, November 5, 2006.

[14] Cable Europe, *"Cable TV Subscribers, Statistics by Cable Europe,"* www.cableeurope/index.php?pid=135.

[15] CIIP, "International Critical Information Infrastructure Protection (CIIP) Handbook 2004, An Inventory and Analysis of Protection Policies in Fourteen Countries," Swiss Federal Institute of Technology, p. 345.

[16] CIGRE International Council on Large Electric Systems, *"Electric System Vulnerabilities: the crucial role of information & communications technologies in recent blackouts,"* Electra, No. 223, December 2005,Copyright 200, www.cigre.org.

[17] Commission of the European Communities, *"On a European Programme for Critical Infrastructure Protection,"* Green Paper, Brussels, 17.11.2005, COM(2005) 576 final.

[18] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, *"A Strategy for a Secure Information Society - 'Dialogue, partnership and empowerment',"* Brussels, 31 May 2006.

[19] Communication from the Commission to the Council, The European Parliament, the European Economic And Social Committee And The Committee Of The Regions; *"A strategy for a Secure Information Society, "Dialogue, partnership and empowerment,"* COM(2006) 251;ec.europa.eu/information_society/doc/com2006251.pdf.

[20] Communication from the Commission to the Council, The European Parliament, the European Economic And Social Committee And The Committee Of The Regions; *"On the Review of the EU Regulatory Framework for electronic communications networks and services. IMPACT ASSESSMENT,"* SEC(2006) 817; europa.eu.int/information_society/policy/ecomm/doc/info_centre/public_consult/review/impactassessment_final.pdf.

[21] Communication from the Commission to the Council, The European Parliament, the European Economic And Social Committee And The Committee Of The Regions; *"On the Review of the EU Regulatory Framework for electronic communications networks and services. Proposes Changes,"* SEC(2006) 816; europa.eu.int/information_society/policy/ecomm/doc/info_centre/public_consult/review/staffworkingdocument_final.pdf.

[22] Communication from the Commission to the Council, The European Parliament, the European Economic And Social Committee And The Committee Of The Regions; *"On the Review of the EU Regulatory Framework for electronic communications networks and services,"* SEC(2006) 334 final, europa.eu.int/information_society/policy/ecomm/doc/info_centre/public_consult/review/com334_en.pdf.

[23] Council Meeting, Council of the European Union, *"Transport, Telecommunications and Energy,"* 2272nd Press Release, Brussels, 11-12 December 2006.

[24] EICTA, *"EICTA comments to the Commission Green Paper on a European Programme for Critical Infrastructure protection,"* www.eicta.org/index.php?id=34&id_article=71.

[25] ECTA, *"Broadband Penetration in EU: The Haves and the Have Nots," 14 September 2006,"* www.ectaportal.com/en/upload/File/Broadband%20Scorecards/Q106/FINAL%20BB%20ScQ106%20Press%20release%20Sept%2006.pdf.

[26] ECTA , *"ECTA Broadband Scorecard End of 2005,"* www.ectaportal.com/en/upload/File/Broadband%20Scorecards/Q405/Broadband%20Scorecard%20Q405.pdf.

[27] ECTA, *"ECTA Scorecards,"* www.ectaportal.com/en/basic245.html.

[28] European Commission; *"Green paper on a European programme for critical infrastructure Protection,"* COM(2005) 576 final; eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf.

[29] European Commission, *"Press Release IP/06/701,"* europa.eu/rapid/pressReleasesAction.do?reference=IP/06/701&type=HTML&aged=0&language=EN&guiLanguage=en.

[30] European Network and Information Security Agency (ENISA), www.enisa.eu.int .

[31] Federal Communications Commission (FCC), *"Report and Order and Further Notice of Proposed Rulemaking, Revision of the Commission's Rules to Ensure Compatibility With Enhanced 911 Emergency Calling Systems,"* FCC 96-264, adopted June 12, 1996, p. 8.

[32] Federal Communications Commission (FCC) Network Reliability and Interoperability Council, <www.nric.org>.

[33] Federal Communications Commission (FCC) Network Reliability and Interoperability Council VI, *"Homeland Security – Physical Security (Focus Group 1A) – Prevention Report, Issue 1, Dec. 2002,"* p. 27, <www.nric.org/fg/nricvifg.html>.

[34] Federal Communications Commission (FCC) Network Reliability and Interoperability Council VI, *"Homeland Security – Physical Security (Focus Group 1A) – Prevention and Restoration Report, Issue 2, Mar. 2003,"* pp.27, 41, <www.nric.org/fg/nricvifg.html>.

[35] Federal Communications Commission (FCC) Network Reliability and Interoperability Council VI, *"Homeland Security – Physical Security (Focus Group 1A) – Final Report, Issue 3, Dec. 2003,"* <www.nric.org/fg/nricvifg.html>.

[36] Federal Communications Commission (FCC) Network Reliability and Interoperability Council VII, *"Focus Group 3A – Wireless Network Reliability – Final Report, Issue 3, Sept. 2005,"* <www.nric.org/fg/index.html>.

[37] Federal Communications Commission (FCC) Network Reliability and Interoperability Council VII, *"Focus Group 3B – Public Data Network Reliability – Final Report, Issue 3, Sept. 2005,"* <www.nric.org/fg/index.html>.

[38] Adrian Fielding, Honeywell, *"The third EU Commission critical infrastructure protection seminar. Meeting report."*

[39] D. Fowler, *"Virtual Private Networks: Making the Right Connection,"* Morgan Kaufman, San Francisco, CA, 1999.

[40] Luisa Franchina, et. al., *"Quality of Service in ICT Networks,"* Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, March 2005.

[41] Luisa Franchina, et. al., *"Network Security from Risk Analysis to Protection Strategies,"* Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, March 2005.

[42] Luisa Franchina, et. al., *“Network Security in Critical Infrastructures,”* Istituto Superiore delle Comunicazioni e delle Tecnologie dell’Informazione, March 2005.

[43] T. H. Grubesic, M.E. O’Kelley, A.T. Murray, *“A Geographic Perspective on Commercial Internet Survivability,”* Telematics and Infomatics, 2003, 20:51-69.

[44] T. H. Grubesic, A. T. Murray, *“Vital Nodes, Interconnected Infrastructures, and the Geographies of Network Survivability,”* Annals of the Association of American Geographers, 2006.

[45] David J. Houck, Eunyoung Kim, Gerard P. O'Reilly, David D. Picklesimer, Huseyin Uzunalioglu, *"A Network Survivability Model For Critical National Infrastructure,"* Bell Labs Technical Journal, Volume 8, Number 4, October 2003.

[46] Internet Crime Complaint Center (IC3), *“2005 Internet Crime Report,”* prepared by the National White Collar Crime Center and the Federal Bureau of Investigation.

[47] IDC, *“Survey of ASP Infrastructure Systems Software,”* 2000.

[48] IDC, *“Western European Hotspot LAN Equipment Forecast,”* 2005-2010.

[49] Institute of Electrical Engineering (IEEE), *“IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries,”* New York, NY: 1990.

[50] IEEE, *“Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop,”* www.comsoc.org/~cqr.

[51] IEEE Communications, Quality and Reliability (CQR), *“Proceedings of European Experts Workshop on Power & Environment,”* Rome Italy, 3 October 2006, www.comsoc.org/~cqr/Docs/Events/EU-Workshop/W1%20Proceedings.pdf.

[52] IEEE Communications, Quality and Reliability (CQR), *“Proceedings of European Experts Workshop on Network & Payload,”* London UK, 6 October 2006, www.comsoc.org/~cqr/Docs/Events/EU-Workshop/WORKSHOP%202%20PROCEEDINGS%20-%20Network%20&%20Payload.pdf.

[53] IEEE Communications, Quality and Reliability (CQR), *“Proceedings of European Experts Workshop on Hardware & Software,”* Berlin, Germany, 11 October 2006, www.comsoc.org/~cqr/Docs/Events/EU-Workshop/W3%20HWSW%20Berlin%20proceedings.pdf.

[54] IEEE Communications, Quality and Reliability (CQR), *“Proceedings of European Experts Workshop on Policy & Human,”* Brussels, Belgium, 15 November 2006, www.comsoc.org/~cqr/Docs/Events/EU-Workshop/W4%20Policy%20&%20Human%20Brussels%20Proceedings.pdf.

[55] IEEE Communications, Quality and Reliability (CQR), *“The Trust Paradigm: Implementing Trusted Methods in Information Technology Management and Security,”* Washington DC, 17 October 2006, www.comsoc.org/~cqr/TrustParadigm-2006.html.

[56] Infonetics Research, *“WiMAX and Outdoor Mesh Equipment, Quarterly Worldwide Market Share Forecasts for 2Q06,”* August 2006.

[57] In-Stat, “*Global VoIP Has Arrived; Just Not As Expected!”* December 2005.

[58] In-Stat, *"Carrier NGN Migration Strategies Set VoIP Market Timing,"* April 2005.

[59] International Organization for Standardization, *"Information Technology–Open Systems Interconnection–Basic Reference Model: The Basic Model,"* ISO/IEC Standard 7498-1, 1994.

[60] International Standards Organization, *"Information Technology - Security Techniques - IT Network Security - Part 2: Network Security Architecture,"* ISO/IEC 18028-2: September 2005.

[61] International Telecommunication Union (ITU), Telecommunication Standardization Sector, *"Security Architecture for Systems Providing End-to-End Communications,"* ITU-T Rec. X.805, October 2003.

[62] International Telecommunication Union, Telecommunication Standardization Sector, "*Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications,"* ITU-T Rec. X.800, 1991.

[63] Internet World Stats, *"Internet Usage in Europe,"* www.internetworldstats.com/stats4.htm.

[64] A. Jrad, T. Morawski, L. Spergel, *"A Model for Quantifying Business Continuity Preparedness Risks for Telecommunications Networks,"* Bell Labs Technical Journal Volume 9, Number 2, 2004.

[65] Ahmad Jrad, Huseyin Uzunalioglu, David J. Houck, Gerard O'Reilly, Stephen Conrad, Walt Beyeler *"Wireless and Wireline Netowrk Interactions in Disaster Scenarios,"* Milcom 2005, October 2005.

[66] A. Macwan, *"Approach for Identification and Analysis of Human Vulnerabilities in Protecting Telecommunications Infrastructure,"* Bell Labs Technical Journal, 9:2 (2004), 85–89.

[67] A. McGee, S. R. Vasireddy, C. Xie, D. Picklesimer, U. Chandrashekhar, and S. Richman, *"A Framework for Ensuring Network Security,"* Bell Labs Technical Journal, Volume 8, Issue 4 , Pages 7 – 27, February 5, 2004.

[68] J. T. McKelvey, "*Combatting Security Risks on the Cable IP Network,"* IBC 2002 Conference, www.broadcastpapers.com/ibc2002/ibc2002.html .

[69] B. L. Malone III, *"Wireless Search and Rescue: Concepts for Improved Capabilities,"* Bell Labs Technical Journal, 9:2 (2004), 34–49.

[70] Mary Meeker, Brian Pitz, Brian Fitzgerald, Richard Ji, *"Internet Trends,"* October 12, 2005, Morgan Stanley, www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends1005.pdf.

[71] Meridian, www.meridian2006.org .

[72] National Security Telecommunications Advisory Committee (NSTAC), "Next Generation Networks Task Force Report," 2006, www.ncs.gov/nstac/reports/2006/NSTAC%20Next%20Generation%20Networks%20 Task%20Force%20Report.pdf.

[73] Network Reliability Steering Committee (NRSC), *"Network Reliability Steering Committee Annual Report, 2001,"* www.atis.org/NRSC/Docs/2001rpt.pdf.

[74] Network Reliability Steering Committee (NRSC), *“Procedural Outage Reduction: Addressing the Human Part,”* May 13, 1999.

[75] PacketCable, Requirements Pkt-tr-voipar-v01-001128, www.packetcable.com.

[76] Pyramid Research, *“Western Europe Fixed Communications Demand,”* June 2006.

[77] Pyramid Research, *“Central and Eastern Europe Fixed Communications Demand,”* June 2006.

[78] Gerard O'Reilly, Thomas Morawski, and Paul Gagen, *"Disaster Recovery/Business Continuity Planning in a New Age,"* Networks 2002.

[79] Gerard P. O'Reilly, David J. Houck, Eunyoung Kim, Thomas B. Morawski, David D. Picklesimer, Huseyin Uzunalioglu, *"Infrastructure Simulations of Disaster Scenarios,"* Networks 2004, Vienna, Austria.

[80] G. O'Reilly, D. Houck, F. Bastry, A. Jrad, H.Uzunalioglu, W. Beyeler, T. Brown, S. Conrad, *"Modelling Interdependencies between Communications and Critical Infrastructures,”* presented at R&D Partnerships in Homeland Security, April 27, 2005.

[81] Gerard O'Reilly, Huseyin Uzunalioglu, Stephen Conrad, Walter Beyeler, *"Inter-Infrastructure Simulations across Telecom, Power, and Emergency Services,"* 5th International Workshop on Design of Reliable Communication Networks, October 16, 2005.

[82] K. R. Rauscher, R. E. Krock, J. P. Runyon, *“Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security,”* Bell Labs Technical Journal, 11(3), 73-78 (2006) ©Lucent Technologies Inc. Published by Wiley Periodicals Inc. Published online at Wiley Interscience (www.interscience.wiley.com) DOI 10.1002/bltj.20179.

[83] K. F. Rauscher, *“Protecting Communications Infrastructure,”* Bell Labs Technical Journal, Volume 9, Number 2 (2004), 1–4 ©Lucent Technologies Inc.

[84] Patrick R.W. Roe (ed), *“Towards an inclusive future (Impact and wider potential of information and communication technologies)”* EUR: 22562 ISBN: 92-898-0027, © COST 219ter, 2007. Published by CST, Brussels. COST is supported by the EU RTD Framework Programme.

[85] SDA roundtable, “*Defending Europe's vulnerable infrastructure,”* www.securitydefenceagenda.org/conferences_ataglance.asp?ConfId=344

[86] D.P. Sieworek and R.S. Swarz, *“Reliable Computer Systems: Design and Evaluation,”* Digital Press, Burlington, MA, 1992.

[87] Strategic Analytics, *“Wireless Operation Outlook 2006,”* January 2006.

[88] Strategic Analytics, *“Western European Cellular User Forecasts, 2005-2010,”* January 2006.

[89] Telcordia Technologies, *“Generic Requirements for Network Elements,”* www.telcordia.com.

[90] The Register, *"While Stealing Bandwidh,"* www.theregister.co.uk/2006/08/29/aol_wireless_survey/ .

[91] United States, Department of Homeland Security, *"Strategic Plan,"* Feb. 23, 2004, www.dhs.gov/interweb/assetlibrary/DHS_StratPlan_FINAL_spread.pdf .

[92] United States, Office of Homeland Security, *"National Strategy for Homeland Security, July 2002,"* <www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf>.

[93] United States, Office of Homeland Security, *"National Strategy for Homeland Security, July 2002,"* pp. vii–viii, <www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf>.

[94] US-Canada Power System Outage Task Force, *"Final Report on the August 14,2003 Blackout in the United States and Canada: Causes and Recommendations,"* April, 2004.

[95] Warning, Advice and Reporting Point (WARP), www.warp.gov.uk.

[96] Wireless Emergency Response Team, *"Wireless Emergency Response Team (WERT) Final Report for the September 11, 2001 New York City World Trade Center Terrorist Attack,"* WERT, Oct. 2001, <www.wert-help.org/WERT-Final-Report.pdf >.

[97] Yankee Group, *"How Big Is Threat of Disruptive IP-Based Wireless Technologies to Mobile Operators?,"* March 2006.

[98] Yankee Group, *"3G's Role in an Increasingly Competitive Wireless Marketplace,"* June 2006.

[99] Yankee Group, *"Wi-Fi and Cellular FMC Solutions Lack Market Acceptance by Nathan Dyer,"* July 18, 2006.

[100] Yankee Group, *"Xfera Can Succeed in Spain with the Right 3G Strategy,"* Aug 30th, 2006.

[101] ZDnet, *"Paris Planning for Citywide Wi-Fi"*, July 4, 2006 news.zdnet.com/2100-1035_22-6090503.html and

[102] ZDnet Government, government.zdnet.com/index.php?page_id=1816&id=1360802