COUNCIL OF THE EUROPEAN UNION

Brussels, 2 April 2009

8375/09
ADD 2

TELECOM 69
DATAPROTECT 24
JAI 192
PROCIV 46

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	31 March 2009
to:	Mr Javier SOLANA, Secretary-General/High Representative
Subject:	Commission Staff Working Document accompanying document to the Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" Impact Assessment (Part 2)

Delegations will find attached Commission document SEC(2009) 399.

Encl.: SEC(2009) 399

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 30.3.2009
SEC(2009) 399

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on Critical Information Infrastructure Protection
"Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience"

IMPACT ASSESSMENT (Part 2)

{COM(2009) 149 }
{SEC(2009) 400}

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).[1] 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

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

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.

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.

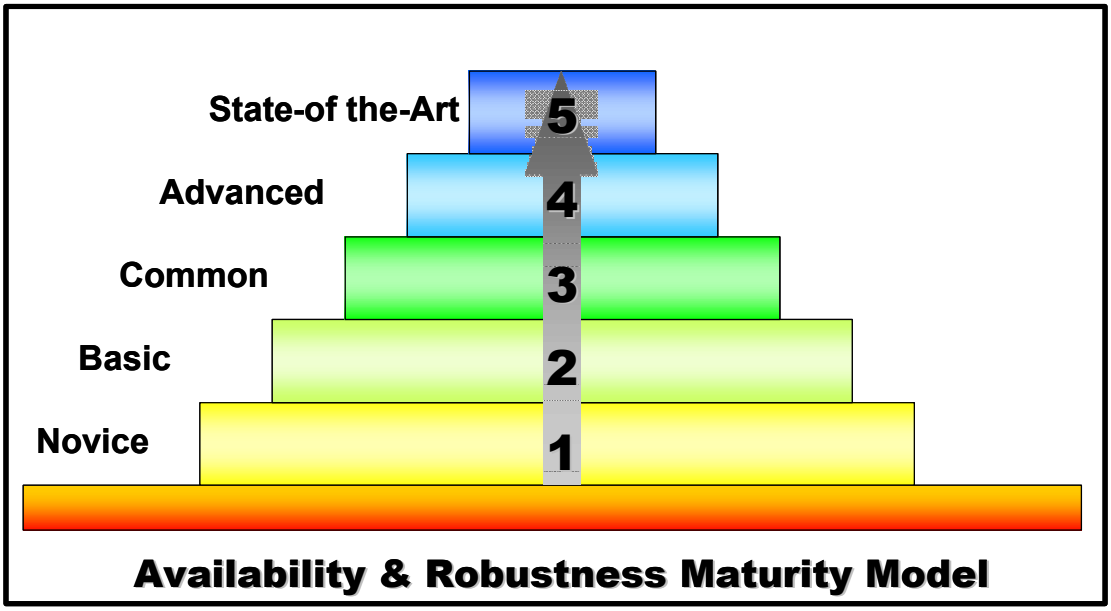


Figure 1: Availability and Robustness Maturity Model

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[2] 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.

[2] *Scope*, Section 2.2.

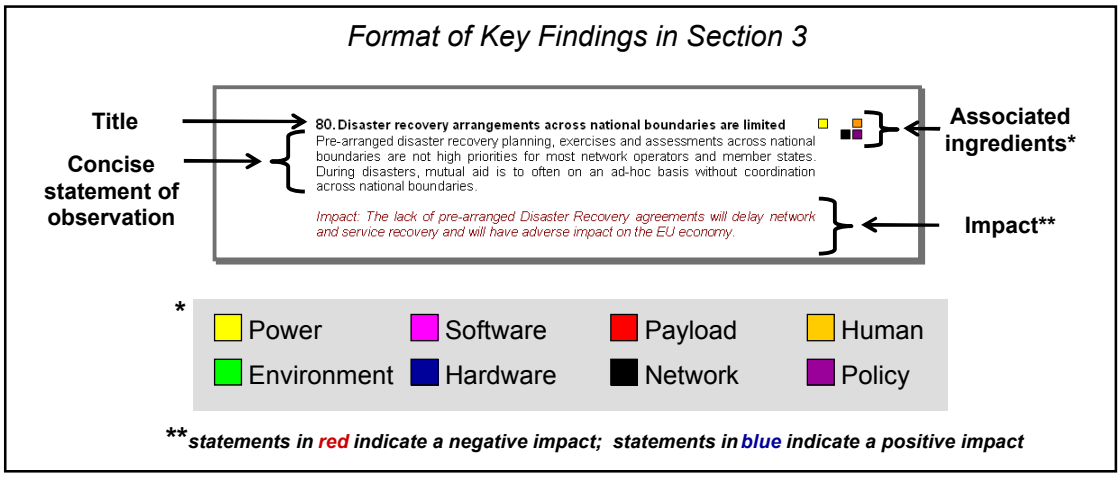


Figure 2: Presentation of Key Findings

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[3]

[3] 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.

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. 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.[4] 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.

[4] 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.[5] 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.[6]

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

[5] A 'Top Concern" from the Proceedings of IEEE CQR, *"Proceedings of European Experts Workshop on Power & Environment,"* Rome Italy, 3 October 2006.
[6] 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.[7] 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.[8]

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

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

Each of the many promised capabilities and anticipated new services will be achieved through the implementation of new software, and sometimes new hardware.[9] 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[10] 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).[11]

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

[9] 2006 European Experts Workshop on Hardware & Software, Proceedings, slide 16, www.comsoc.org/~cqr/EU-Proceedings-2006.
[10] The introduction of new software versions also holds the possibility of introducing new problems and incompatibilities with prior implementations.
[11] 2006 European Experts Workshop on Power & Environment, Issues Voting, slides 9-10, www.comsoc.org/~cqr/EU-Proceedings-2006.

interfaces.[12] 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.[13]

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,[14, 15] 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". [16, 17]

12 2006 European Experts Workshop on Hardware & Software, Proceedings, slide 17, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
13 2006 European Experts Workshop on Power & Environment, Issues Voting, slides 4-5, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
14 90% of subject matter experts confirm. Proceedings of the Power and Environment Experts Workshop, Rome, Italy, October 3, 2006. www.comsoc.org/~cqr.
15 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.
16 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.
17 100% 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.[18]

[18] 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[19] 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.[20]

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.

[19] 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).
[20] 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.[21] 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.[22]

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.

[21] 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.
[22] 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.[23]

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.[24, 25] 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.[26]

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

[23] 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.
24 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.
[25] 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.
[26] 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.[27] 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.[28] 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.

[27] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 9, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[28] 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[29] are providing access to government services and databases, and network access to the public, but do not have a "security culture".[30] 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.[31]

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).

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

[30] 2006 European Experts Workshop on Power & Environment, Proceedings, slide 12, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[31] 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.[32] 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.[33]

[32] Standards are being developed for service emulation (i.e. same functionality and operation) and service simulation (i.e. equivalent functionality, operation may differ).
[33] 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.[34] These Best Practices deal with each of the eight ingredients of communications infrastructure.[35]

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.[36] Incumbents in the market place tended to have higher implementation levels compared to new entrants.

[34] 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.

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

[36] 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[37]) 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[38] 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.

[37] A malicious attempt to render a computer resource unavailable to its intended users.

38 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[39] 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.[40] 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,[41] but are not being sufficiently utilised

Periodic testing of emergency plans is not a common practice for most network operators.[42] 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.

39 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.

[40] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 11, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[41] 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.

[42] 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[43]). 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.[44]

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.

[43] CAC is further discussed in Annex E.
[44] 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.[45] These include general lowered levels of control, reduced access to the developers and exposure to programmer loyalties.[46] In addition, timeframes for program fixes are less predictable.[47]

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.[48, 49, 50]

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

45 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.
[46] 2006 European Experts Workshop on Hardware & Software, Issues Voting, slides 18-19, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[47] 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.
48 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.
[49] 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.
[50] 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[51] as one moves among, and accesses, different networks. As these networks can deploy different technologies,[52] the hand-offs for these active sessions require nontrivial coordination.[53]

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.[54] This can be accomplished by requiring security measures for interaction with government services, providing public security awareness training, and funding security initiatives.[55]

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.[56]

[51] a session includes a voice call, video or other application.
[52] e.g., WiFi, WiMAX, and 3G.
[53] 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.
[54] 2006 European Experts Workshop on Power & Environment, Proceedings, slide 15, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[55] 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.
[56] 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.[57, 58, 59]

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.[60]

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,[61] will be needed to allow for identity management across network security domains.[62]

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

[57] 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.
[58] 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.
[59] 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.
[60] 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.
[61] 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.
[62] 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).[63]

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.[64]

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.[65, 66]

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.

[63] 2006 European Experts Workshop on Network & Payload, Proceedings, slide 25, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[64] 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.
[65] 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.
[66] 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.[67]

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.[68]

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.

[67] 2006 European Experts Workshop on Hardware & Software, Proceedings, slide 20, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

[68] 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[69] 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.[70]

[69] 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.

[70] 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.[71]

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).[72]

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.[73] In addition to the participation of several network operators simultaneously in most markets, the United States has learned from several recent crises that spanned

[71] 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.
[72] 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.
[73] 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.[74]

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.[75]

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.[76] 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.

[74] IETF Pre-Congestion Notification Working Group (PCN) is developing a standard.
[75] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 16, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[76] 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.[77]

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.[78] 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.[79] 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[80] 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

[77] 2006 European Experts Workshop on Network & Payload, Proceedings, slide 24, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[78] This is accomplished by Signalling System 7 (SS7) out-of-band signalling.
[79] 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.
[80] For example, IPSec, end-user identification and authentication.

hosts best-in-class information sharing programs.[81] 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).[82] 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.[83] 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.*

[81] Warning, Advice and Reporting Points (WARPs) and National Infrastructure Security Coordination Centre (NSCC).
[82] 2006 European Experts Workshop on Network & Payload, Proceedings, slide 25, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[83] 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.

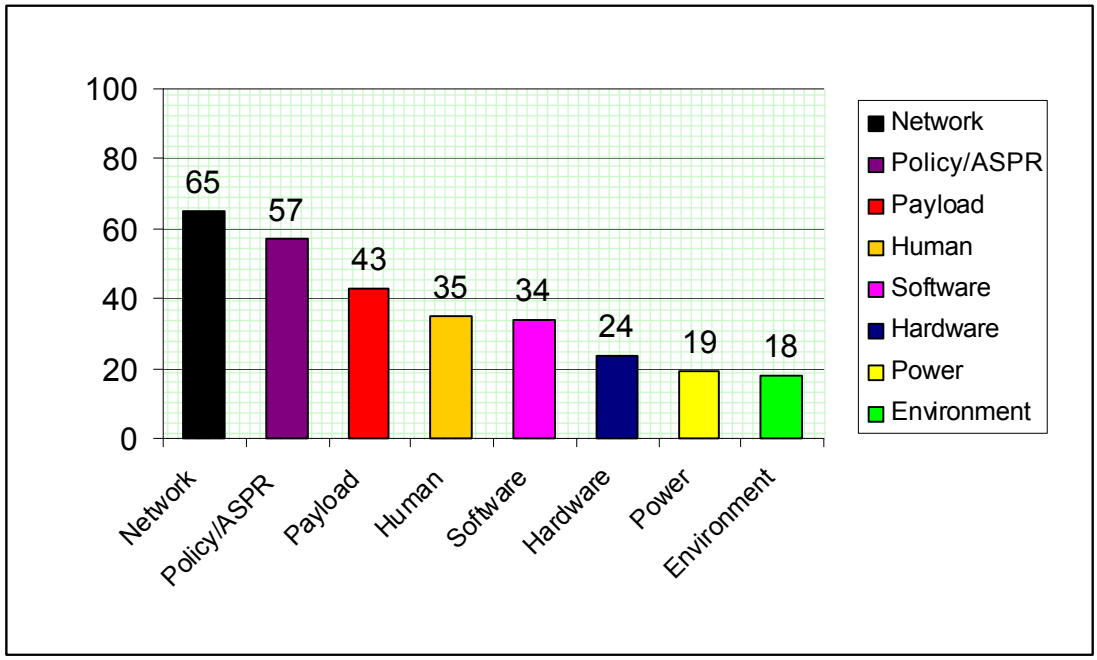


Figure 3: Summary of Key Finding Association with Eight Ingredients

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.[84]

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 1: 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*

[84] 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.[85]

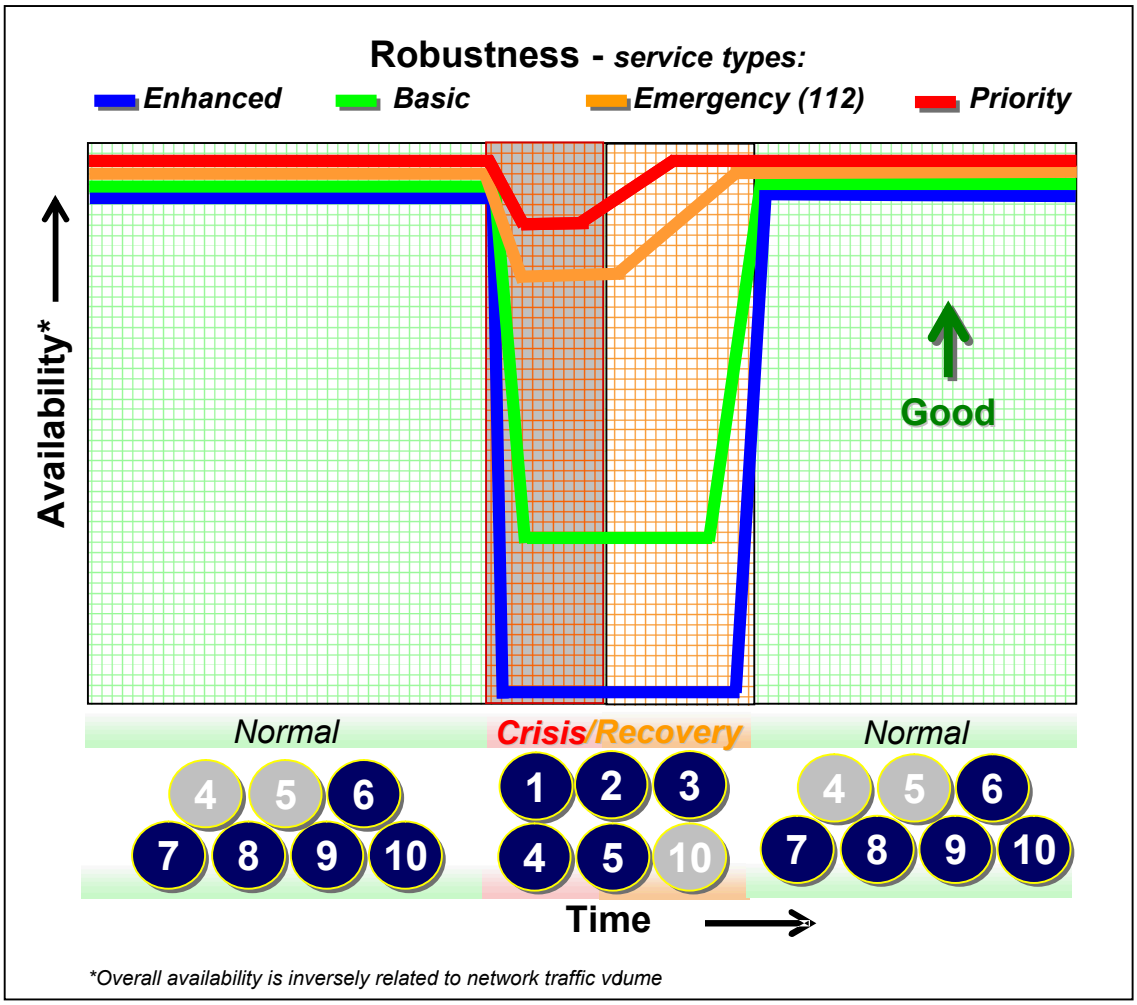


Figure 4: Impact of Recommendations in Relation to Infrastructure Stress Event

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.

[85] 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.[86] 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.

[86] *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.

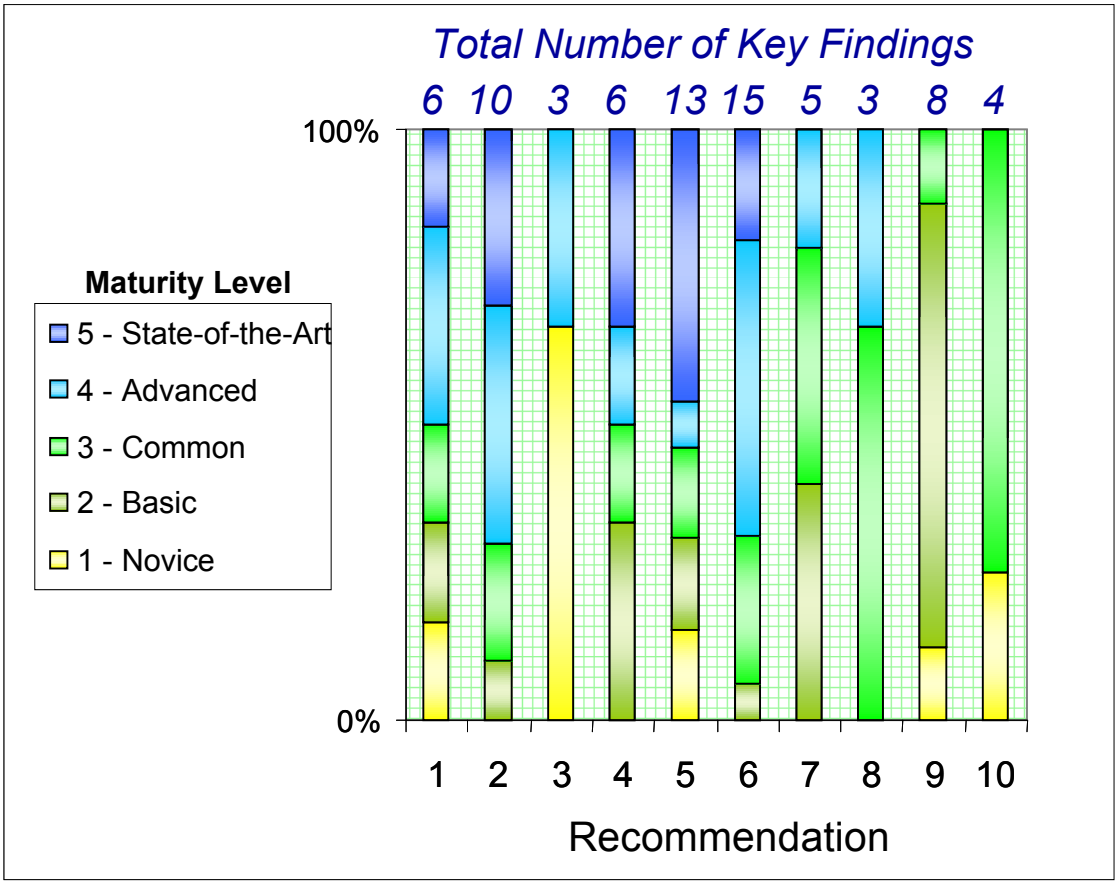


Figure 5: Recommendation References to Key Finding Maturity Levels

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.[87,88] *While some network operators, service providers and government stakeholders do conduct periodic emergency preparedness exercises, others have made very limited investment in this area.*[89, 90, 91] *In many cases, most often with new entrants, the preparedness plans are mostly informal and lack structure.*[92] *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.*[93]

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,[94] 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.[95, 96]

(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.

[87] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 6, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[88] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 2, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[89] Key Finding 18, The level of emergency preparedness varies greatly across Europe, Section 3.2
[90] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 3, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[91] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 7, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[92] Key Finding 3, Emergency Preparedness is largely informal, Section 3.1.
[93] Priority restoration of communications circuits was critical for the Wall Street Financial District following the September 11, 2001 terrorist attacks.
[94] Key Finding 60, Emergency exercises are essential in preparing for disasters, but are not being sufficiently utilised, Section 3.4.
[95] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 10, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[96] International CIIP Handbook 2006, Volume II, "Sectors and Beyond: Analyzing what is Critical" page 31, Center for Security Studies, ETH Zurich.

(c) The Private Sector and Member State Governments must conduct emergency exercises that include additional infrastructures and actively 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.[97]

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[98]) improves the availability of communications services,[99] 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.

[97] Key Finding 29, Priority restoration for critical subscribers is not commonly supported, Section 3.3.
[98] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 11, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[99] 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.[100]

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.[101] 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.

[100] Key Finding 84, Disaster recovery arrangements across national boundaries are limited, Section 3.5.
[101] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 9, www.comsoc.org/~cqr/EU-Proceedings-2006.html.

4.2 Priority Communications[102] on Public Networks

Background

During disaster situations, whether natural or manmade, certain communications are simply essential for saving lives and property as recovery occurs.[103] 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.[104]

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.[105]

d) As primary stakeholders for such a capability, Member State governments must fund its development, implementation and ongoing maintenance.[106]

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

[102] 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).
[103] Key Finding 28, Priority calling for critical communications in public networks is needed. Section 3.3.
[104] Key Finding 56, IP-based emergency communications services have not been deployed. Section 3.4.
[105] Key Finding 86, Priority communications mechanisms are needed between Member States. Section 3.5.
[106] 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.[107] While these networks have proven valuable and should be maintained, an emergency scheme[108] 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.[109]

Achieving priority on future networks will be more challenging than on a legacy network due to the complexity of bandwidth management,[110] the various types of services supported[111, 112] and the authorisation issues.[113]

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[114] descriptions for priority calling.

[107] Key Finding 85, Several Member States have completely separate communications networks for critical functions. Section 3.5.
[108] Key Finding 51, Net Neutrality may be misunderstood. Section 3.3.
[109] Key Finding 87, Validation of user authorisation to place priority emergency calls does not address inter-network calls. Section 3.5.
[110] Key Finding 64, Many network operators do not prioritise packets. Section 3.4.
[111] 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.
[112] Key Finding 57, Future networks have the opportunity to introduce mechanisms for early warning services. Section 3.4.
[113] Key Finding 55, Authorisation of priority communications users must be managed. Section 3.4.
[114] 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 States.

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:[115] 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.[116]

Inter-Member State priority calling deployed: Priority calls between Member States' networks are supported.

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.
[115] European stakeholders participated in the creation of the standards and are comfortable that it meets European needs.
[116] 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.[117] *However, while there are some few exceptions, mutual aid in Europe is not widely practiced.*[118] *Further, when mutual aid is practiced, it is largely ad hoc and susceptible to failure – especially during times of stress.*[119, 120]

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.[121]

(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).[122]

[117] 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.
[118] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 6, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[119] Key Finding 3, Emergency preparedness is largely informal, Section 3.1
[120] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 8, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[121] Key Finding 4, Future network operators may not be recognised as part of the critical infrastructure, Section 3.1.
[122] 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.

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

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.[123] 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.[124, 125] 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.

[123] Key Finding 58, Mutual aid agreements are essential for effective incident response, Section 3.4.
[124] 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).
[125] 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.

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

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.[126, 127] 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.[128] 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.[129, 130]

(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.[131, 132, 133]

(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.[134]

[126] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 8, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[127] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 3, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[128] Key Finding 19, Emergency information sharing during incidents is limited, Section 3.2
[129] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 7, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[130] 2006 European Experts Workshop on Power & Environment, Issues Voting, slide 2, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[131] 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..
[132] Key Finding 35, Dialogue within the industry is limited, Section 3.3.
[133] Key Finding 89, Collaboration between stakeholders in the U.S. is perceived to be more mature than in Europe, Section 3.5.
[134] Key Finding 19, Emergency information sharing during incidents is limited. Section 3.2.

(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[135] 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.

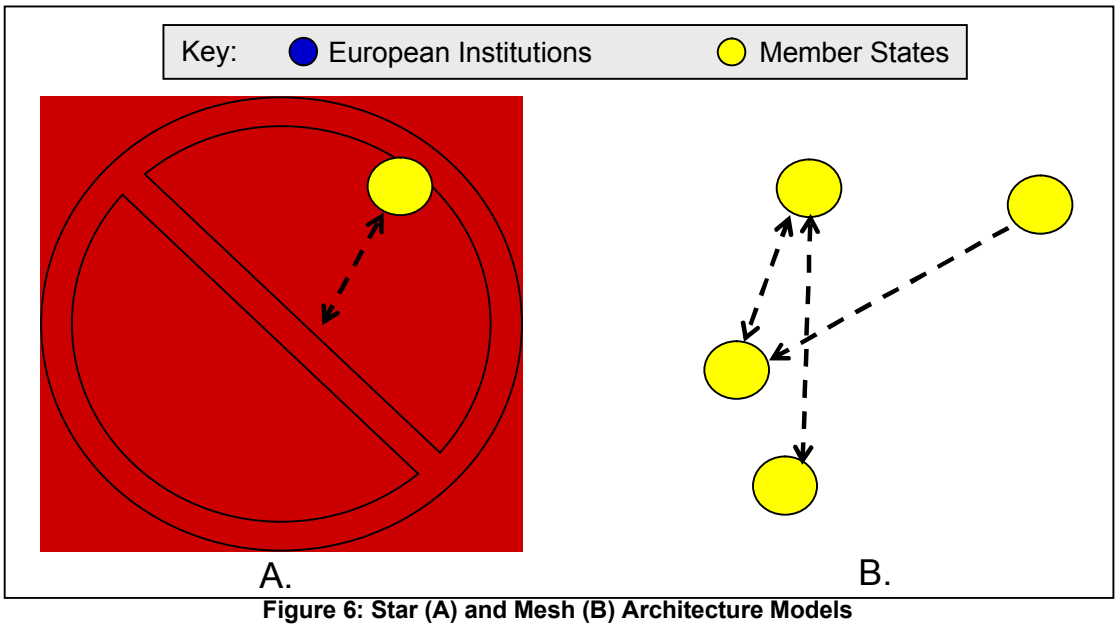


Figure 6: Star (A) and Mesh (B) Architecture Models

[135] 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,[136, 137, 138] learning their methods[139] 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:

[136] Key Finding 98, Europe has positive information sharing role models, Section 3.5.
[137] NISCC, www.niscc.gov.uk/niscc/index-en.html.
[138] International CIIP Handbook 2006, Volume I, "Information Sharing and Analysis Centres (ISAC)" page 329, Centre for Security Studies, ETH Zurich.
[139] 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[140, 141] and the European Institutions.[142] 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[143, 144] they may have a European-wide impact.[145]

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[145,146] 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.[147, 148, 149]

(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.[150]

[140] 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.
[141] International Critical Information Infrastructure Protection Handbook 2006, Volume 2, "Analyzing Issues, Challenges, and Prospects," Center for Security Studies, ETH Zurich.
[142] Green Paper, On a European Programme for Critical Infrastructure Protection, Commission of the European Communities, COM(2005) 576 final, Brussels, BE, 17 November 2005.
[143] Key Finding 40, Agreements, standards, policies and regulations (ASPR) are Member State dependent, Section 3.3.
[144] Key Finding 41, Local governments play a critical role in maintaining the reliability and security of networks, Section 3.3.
[145] 2006 European Experts Workshop on Power & Environment, Top Concerns 3, 5, 11, , slides 10, 12, 15, (www.comsoc.org/~cqr/EU-Proceedings-2006).
[146] Key Finding 4, Future network operators may not be recognised as part of the critical infrastructure. Section 3.1.
[147] Key Finding 89, Collaboration between stakeholders in the U.S. is perceived to be more mature than in Europe. Section 3.5.
[148] 2006 European Experts Workshop on Power & Environment, Top Concern 13, , slide 10, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[149] 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[151, 152] (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.[153]
- *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,[154, 155] including those crossing national boundaries
B. prioritise each of these interdependencies
C. create a functional map[156, 157, 158, 159, 160] of the critical aspects[161] of the highest priority interdependencies in order to better prepare for, and mitigate against, the impacts of a natural or manmade threat

---

[150] 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.
[151] Key Finding 84, Disaster recovery arrangements across national boundaries are limited. Section 3.5.
[152] Key Finding 91, Minimal network management information is shared between broadband network operators and access service providers. Section 3.5.
[153] Key Finding 86, Priority communications mechanisms are needed between Member States. Section 3.5.
[154] Key Finding 92, There is minimal information sharing between critical sectors. Section 3.5.
[155] Key Finding 98, Europe has positive information sharing role models. Section 3.5.
[156] 2006 European Experts Workshop on Hardware & Software, Top Concerns 16, 33, slides 13, 15, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[157] 2006 European Experts Workshop on Policy & Human, Top Concern 23, slide 18, 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[162,163,164] 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:[165, 166]

> **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.

[158] 2006 European Experts Workshop on Power & Environment, Top Concern 9, slide 10, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[159] Key Finding 19, Emergency information sharing during incidents is limited. Section 3.1.
[160] Key Finding 59, Critical communications infrastructures lack restoration agreements. Section 3.4.
[161] For example, ownership, 24-hour emergency contact information, expectations for restoral procedures, priority restoration programs, incident reporting procedures.
[162] Key Finding 26, The Private Sector is not treated by government as an equal partner. Section 3.2.
[163] 2006 European Experts Workshop on Policy and Human, Top Concern 7, slide 17, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[164] 2006 European Experts Workshop on Policy & Human, Top Concern 28, slide 19, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[165] 2006 European Experts Workshop on Policy & Human, Top Concern 14, slide 18, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[166] 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.[167, 168] Future networks will consist of many more network elements[169] with many of these elements consisting of outsourced components supplied by both new and established equipment suppliers.[170] Many of these components will utilise common hardware and software modules, thereby increasing the potential for single modes of failure or cascading network problems.[171] Further, ensuring the end-to-end security of future networks[172] 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.[173, 174] Existing solutions are not sufficient to address the challenges of future networks.[175, 176] 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

[167] Key Finding 17, Layered software introduces additional complexity, Section 3.2.
[168] Key Finding 76, Third party components may have an adverse impact on networks, Section 3.4.
[169] Key Finding 39, Future networks will be more difficult to manage, Section 3.3.
[170] Key Finding 77, New equipment vendors may have an adverse impact on the supply chain, Section 3.4.
[171] Key Finding 80, Cascading failures of a hardware component or a software element require new management strategies, Section 3.4.
[172] Key Finding 96, End-to-end security is implemented hop-by-hop, Section 3.5.
[173] Key Finding 79, Introduction of network security may impact service availability, Section 3.4.
[174] Key Finding 75, Future networks are more vulnerable to signalling fraud from end-user devices, Section 3.4.
[175] Key Finding 43, Security approaches used by the PSTN/IN are not sufficient for future networks, Section 3.3.
[176] 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).

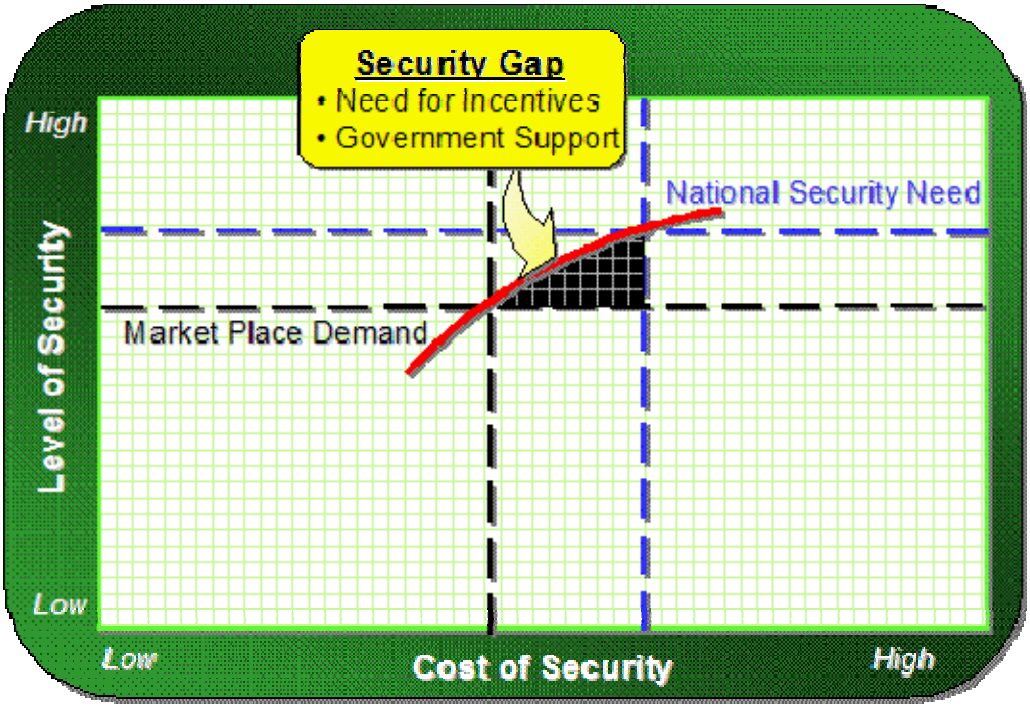


Figure 7: Nation-State Security Needs Exceed Market Place Demands[177]

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.* [178, 179]
- 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.*[180, 181, 182, 183]

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.

[177] NRIC VI Homeland Security Physical Security Final Report, "Meeting NS/EP Security Needs", Issue 3, December, 2003, p.15.
[178] Key Finding 97, Reliability and security practices vary considerably across network operators and service providers, Section 3.5.
[179] Key Finding 74, Federated Identity Management will become a compelling security strategy in future networks, Section 3.4.
[180] Key Finding 50, Future networks contain signalling elements whose failure can cause major outages, Section 3.3.
[181] Key Finding 44, Future networks creates signalling traffic security and reliability challenges, Section 3.3.
[182] Key Finding 67, Future networks provide wider access to network controls, Section 3.4.
[183] 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)[184], 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,[185] or releases of standards,[186] can cause communications to fail or to not work as expected.[187] 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.

[184] Key Finding 40, Agreements, Standards, Policies and Rules (ASPR) are Member State dependent. Section 3.3.
[185] Key Finding 7, Multiple standards bodies are producing different standards. Section 3.2.
[186] Key Finding 13, Future networks require vigilance in upgrading software. Section 3.2.
[187] 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*.[188]

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.

Measures of Success

[188] Key Finding 61, Security integration and interoperability testing guidelines are inconsistent. Section 3.4.

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.[189] *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.[190]

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*.[191] 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[192, 193] 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.*

[189] Key Finding 30, Interconnection testing is not based on a recognised standards-based framework section 3.3.
[190] Key Finding 61, Security integration and interoperability testing guidelines are inconsistent, Section 3.4.
[191] Key Finding 31, Interoperability testing between networks is often an overlooked function section 3.3.
[192] The ATIS PTSC-IOP Technical Report could be used as a starting point for the development of a European IP NNI Testing Framework.
[193] 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.[194, 195] *It is clear that it hasn't been achieved to this point.*[196, 197] *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,*[198] *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.*[199, 200, 201]

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.

(c) The Private Sector, Member States and European Institutions must recognise that this partnership will not be successful without wholehearted commitment from each stakeholder.

[194] Key Finding 19, Emergency information sharing during incidents is limited, Section 3.2.
[195] Key Finding 40, Agreements, Standards, Policies and Regulations (ASPR) are Member State dependent, Section 3.3.
[196] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 15, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[197] 2006 European Experts Workshop on Policy & Human, Issues Voting, slide 16, www.comsoc.org/~cqr/EU-Proceedings-2006.html.
[198] A Google query with the search criteria [ICT Europe government industry partnership] returns over 1 million hits.
[199] Key Finding 21, Collaboration between governments and the Private Sector needs improvement, Section 3.2.
[200] Key Finding 23, Private sector disappointed in yield of government partnerships, Section 3.2.
[201] Key Finding 24, Government regulators are cautious regarding Private Sector claims, Section 3.2.

(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.[202] *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.[203]

9-2. Member States and European Institutions should engage industry representatives to collaborate on studies of identified issues at the *beginning* of a study.[204]

[202] Key Finding 26, The Private Sector is not treated by government as an equal partner, Section 3.2.
[203] Key Finding 25, Companies are not committing expertise in engagements with government, Section 3.2.
[204] Key Finding 5, Government engages network operators too late, Section 3.1.

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?

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.[205] 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.[206]

(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.[207]

[205] Key Finding 52, European communications industry experts confirmed core set of Best Practices, Section 3.3.
[206] Key Finding 53, Private sector implementation of European-confirmed Best Practices is high, Section 3.3.
[207] 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[208] . . . *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/)http:/// are considered as effective or moderately effective by 90% of the European subject matter experts involved.[209]

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.

[208] Key Finding 5, Government engages network operators too late, Section 3.1.
[209] ~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?[210]

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?

[210] 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.[211]

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.

[211] 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 8: 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.

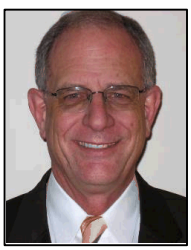
Dr. Himanshu Pant is a distinguished member of technical staff in the High Availability and Security Networks group at Bell Labs. Himanshu has over 15 years of experience in the telecommunications industry concentrating in the areas of system

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.[212]

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.[213]

[212] ATIS Telecom Dictionary. www.atis.org

Reliability
Reliability is simply the likelihood that a system will perform its intended function within the context it was designed to operate within.[214]

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.[215]

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.[216]

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.

---

[213] ATIS Telecom Glossary 2000, T1.523-2001, www.atis.org/tg2k/
[214] 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.
[215] 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.
[216] 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%20Task%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

ANNEX 13: SUMMARY OF THE RESPONSES TO THE EUROPEAN COMMISSION INVITATION TO COMMENT ON THE ARECI STUDY

EUROPEAN COMMISSION
Information Society and Media Directorate-General

Audiovisual, Media, Internet
Internet; Network and Information Security

Brussels, 02 April 2008

WORK PAPER

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

DISCLAIMER

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

CONTENTS

1. OVERVIEW

In the 2006 Communication on "*A strategy for a Secure Information Society – "Dialogue, partnership and empowerment*""[217], the Commission characterised security and resilience of communication networks and information systems as a key policy priority for the European Union (EU). In that context, the European Commission has announced in the *Commission Legislative and Work Programme 2008*[218] a European policy initiative on Critical Information Infrastructure Protection (CIIP). The objective of this initiative, within the broader framework of the European Programme on Critical Infrastructure Protection[219], is to ensure that adequate and consistent levels of **preventive, detection, emergency and recovery measures** are in place. To this end, the European Commission intends to engage relevant stakeholders and to build on national and private sector activities.

As a first step towards an EU policy initiative on CIIP, the European Commission engaged, in 2006, in a study on the *Availability and Robustness of Electronic Communication Infrastructures* (ARECI)[220]. The main findings of this study were presented to a broad audience comprising representatives of governments, industry and users on the 18 January 2007 and later on the Commission invited all interested parties to comment on the study's findings. Sixteen contributions drawing up comments on the ARECI study and its ten recommendations for enhancing the availability and robustness of electronic communication infrastructures have been received from a variety of stakeholders. The respondents include industrial associations in the fields of Telecommunications, Internet Services, Network and Information Security (NIS) and Critical Infrastructure Protection as well as individual operators or providers of electronic communications networks and services, one NIS products and services provider, two Member State authorities, one political party, two European Union specialised centre/agency and a standardisation body.

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

---

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

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

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

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

Comments on the recommendations

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

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

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

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

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

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

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

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

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

2. SUMMARY OF THE COMMENTS RECEIVED

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

2.1. Comments concerning the ARECI study in general

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

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

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

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

Respondents also addressed other issues in their contributions as follows:

- A telecom operator considered that the identification of critical infrastructure should be taken forward by Member States based on uniform criteria established across European Union. Infrastructure interdependencies and vulnerabilities of all the players involved in the implementation of the recommendations should also be identified further.

- A respondent considered that the study is biased against Open Source and noted that ignoring Open Source's benefits to critical infrastructure would be a grave mistake. It was also mentioned that the threats of software monoculture were ignored in the report and information systems warfare issues were not specifically addressed.

- A respondent directly involved in critical infrastructure protection welcomed a strategy for raising awareness for planning and investing on critical infrastructures and emergency response. It also supported measures that would lead to an increased harmonization of disaster recovery arrangements across borders, standards, and general policy and regulatory frameworks. Furthermore it was mentioned that there are niche players willing to offer services needed to fill the gaps identified by the ARECI study in terms of preparedness, resilience and prioritization, arguing against the ARECI report statement that normal market forces are not at play in this area.

2.2. Comments on the recommendations

Recommendation 1 – Emergency Preparedness

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

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

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

Other respondents remarked that joint emergency exercises are just one phase of a Risk Management framework and that most of the value of exercises comes from learning how to get 'people' and 'process' issues right and find unexpected dependencies, rather than from the specifics of the scenario.

A respondent in the field of Internet services showed a sceptical view on the outcomes of the recommendation. First of all, it was not clear to what "critical services" were referred to – whether communications infrastructures or other critical sectors. Secondly, emergency preparedness was considered, to some extent, as part of business continuity

planning and consequently the private sector should be encouraged to develop such plans accordingly. Finally, in its view it was not clear to what extent emergency exercises and priority restoration exercises contribute to the enhancement of robustness. A European body shared the same opinion on the generic approach of this recommendation – there is a need to clearly identify the meaning of emergencies and the role of each stakeholder.

Respondents also raised other issues that are worth noting:

- Who will bear the costs of emergency exercises, especially cross border ones that will require a significant investment;

- EU and Member States should foster Research on Risk Management/Risk Assessment methods to address large dependable systems;

- One respondent noted that this topic is also covered by the Public Safety Europe forum initiatives and therefore its activities should be taken into consideration.

Recommendation 2 – Priority Communications on Public Networks

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

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

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

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

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

Other concerns raised by respondents include:

- The type of priority needed/implemented on public networks should depend on the specifics of the infrastructure involved and the emergency situation;

- A telecom operator drew attention to the fact that the implementation of this recommendation should not represent a financial burden for telecom and network operators and should rather be subsidized by Member States;

- Another respondent pointed out that the recommendation as stated implies that all emergency calls from any stakeholder will be prioritized and if this is put in place as a requirement for the European communications infrastructure, a complex agreement between service providers, equipment suppliers and regulators has to be foreseen on the definition of the networks' architecture and on which networks prioritization should be implement first;

- Other solutions different from implementing priorities on public networks are:

  Creating ad-hoc peer-to-peer public networks;

  Set-up a dedicated emergency network owned by the Member States (even if the operations are delegated to an operator) onto which all operators could connect their operations.

Recommendation 3 – Formal Mutual Aid Agreements

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

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

Therefore, three approaches were proposed. Firstly, a study on the legal implications of such agreements before putting them in place was proposed. Secondly, it was suggested that instead of establishing mutual aid agreements based on abstract definitions of threats and vulnerabilities, preparatory risk and business continuity assessments based on an asset-oriented approach should be carried beforehand in order to create more focused mutual aid agreements. Thirdly, a respondent had put forward that what is needed is a cooperative approach (for instance through the creation of public-private partnerships, communication protocols, information exchange or preparedness/assistance schemes) among industry, government and law enforcement, enabling greater flexibility and scope to develop effective and responsive relationships.

Besides these proposals, telecom operators suggested that Member States should commit the necessary funds to put this recommendation forward and that precise equipment

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

Recommendation 4 – Critical Infrastructure Information Sharing

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

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

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

Two other respondents drew attention to the fact that generally there is willingness to share information but lack of motivation to do so unless there is a clear incentive, especially in the case of higher maturity level stakeholders. Additionally, although two respondents directly involved in NIS activities agreed that a star topology is not appropriate for reasons of trust and could possibly create obstacles, they did not fully agree with a full mesh architecture. One contributor highlighted that an element of European coordination would still be necessary, and the other considered that the number of connections among different infrastructures (and consequently stakeholders) would be an obstacle and would end providing only a partial view of the online threat environment that an operator would have access to. Another respondent also remarked that one-to-one links will most probably never result in effective information sharing and the creation of a new "European Institution" is not the solution to put forward. The need for a common "language" to describe security incidents, response and escalation that can be used across sectors and borders was also pointed out by respondents.

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

Recommendation 5 – Inter-Infrastructure Dependency

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

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

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

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

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

Recommendation 6 – Supply Chain Integrity and Trusted Operations

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

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

Although the other contributors also agreed with the present recommendation, they considered that some risks exist. First, Internet and NIS service providers and an EU public body pointed out that if the recommendation is not designed and applied with great caution it could stifle competition in a free and competitive market and possibly put Europe in competitive disadvantage in relation to worldwide players. Second, having a monoculture in information security for instance could create a single point of failure and

hence have as side effects the reduction of innovation and limitation of choice. Indeed, diversity may actually prove beneficial, since compromised trust or security with one provider would not necessarily have an impact on any other part of the supply chain.

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

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

Recommendation 7 – Unified European Voice in Standards

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

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

The other contributors did not support the recommendation as it is drafted. It was said that such recommendation is contrary to European competition rules and somehow unrealistic because there are several competing fora addressing the same technical issues. A unified EU voice in standards would make standardisation less technical and more political. In fact, while a unified EU voice may create a more simple standards framework for companies, they would still need to comply with international standards if they operate on global markets, resulting in a more complex and confusing standards framework. Therefore, it is neither desirable to complicate the development of standards nor to close the EU market to international third parties. In addition, the establishment of a single standard does not guarantee better security and can actually create a single point of failure. Finally, it was supported that standards development should remain an industry-lead activity, but cooperation between industry and Member States would be advantageous in order to assist EU public policy aims and meet the requirements and needs of Member States .

Recommendation 8 – Interoperability Testing

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

This recommendation was supported by all the contributors except two respondents. However, it was mentioned that the description of the recommendation should be more

detailed in particular in terms of scope and criteria of the testing framework. Although interoperability testing is definitely needed, security aspects such as penetration and vulnerability testing and risk assessment of new networks should be emphasized.

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

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

Recommendation 9 – Vigorous Ownership of Partnering Health

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

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

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

Recommendation 10 – Discretionary European Expert Best Practices

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

All contributors seemed to agree that sharing and using Best Practices is beneficial across the various ICT industry sectors and can serve as a useful tool or basis for further discussions. However, some respondents noted that it will take some time and will be costly to implement such a recommendation. An active intervention of governments and regulators was requested by an operator. According to an association in the field of NIS a trusted and effective information sharing infrastructure will be crucial for the success of

the recommendation. This respondent actually made reference to the existing information sharing framework in the United Kingdom called Traffic Light Protocol. Internet services providers agreed with this recommendation as a way to foster the development of network security. Its implementation should however respect the unique know-how of service and network operators.

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

3. ANNEX – LIST OF CONTRIBUTORS

Table 1 - List of contributors

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

ANNEX 14: SUMMARY REPORT OF THE STAKEHOLDER MEETING ON AVAILABILITY AND ROBUSTNESS OF ELECTRONIC COMMUNICATIONS NETWORKS

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

Brussels, 18 June 2007

Introduction

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

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

Presentation

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

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

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

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

Discussion

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

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

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

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

- There is room and in fact need for a multi-stakeholder dialogue on availability and robustness of electronic communications networks in Europe; this dialogue becomes increasingly urgent because a growing number of Member States is preparing their own approach.

- To this end, it would be useful to do some stock taking i.e. to produce an inventory of who does what in Europe (initiatives in Member States, what public-private-partnership structure and drivers); to (develop mechanisms to) analyse what has been achieved at national level; and to see whether such existing good practices can be and would usefully be replicated at the European level.

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

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

Final remarks

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

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

Annex: Further issues raised

1. Presentations and discussion revealed that different views are held on the model for information sharing in Europe: meshed or central. Where the ARECI report promotes a meshed system, others advocate a centralised system as the only manageable solution in a real time environment.

2. Commentators stressed that once good information sharing mechanisms are in place, then the difference between the governments' interests and firms' own self-interests are small. This strengthens our motivation for multi-stakeholder dialogue in Europe to enhance our shared understanding of the issues.

3. Commentators raised the point that multiple components and network elements, typical for the heterogeneous nature of future networks, place a burden on incumbent network operators. It is increasingly difficult to establish procedures leading to the identification of protection gaps and identify liabilities. A need was identified to develop security metrics via collaborative efforts.

4. It was pointed out that business' continuity plans are based on broadband access but the dimensioning is not compatible with plans and usage in fixed telecommunications covered by the ARECI report. The need for an overall IT risk management approach and an alignment of IT solutions with the risks was highlighted. While the ARECI report provides a complete list of ingredients that make up a communications infrastructure, in the new online environment with multiple levels of complexity security needs to be process driven, proactive, fast, flexibly and intelligence led. Present day organisations are not fast enough to deal with the new environment. Technological developments are taking place at such a fast pace that authorities and other decision making bodies have insufficient up-to-date expertise and information, and these bodies are in danger of implementing measures that are out of step with the actual threat situation

5. Participants said that the ARECI report is technical contents only. They emphasised the critical role of people and processes to make technology works and ensure ongoing effectiveness in the light of both changes in the online threat environment and the adoption of advanced modern technology by the emergency services. Also the importance of cultivating a trusted environment was often mentioned.

6. Although Internet service providers agree on the importance of identity management, they disagree with statements in the ARECI report on the need for federated identity management.

7. Commentators raised new issues such as outsourcing in a multi-vendor hardware/software stack and stressed the dependency on suppliers of equipment and installers. Open source was seen as very important for managing a national crisis.

8. Commentators said that the ARECI report does not cover mobile. But the number of mobile subscribers is twice the number of fixed subscribers while

mobile networks may have special vulnerabilities including failure to power outages. National roaming for emergency service is mentioned as a possible measure to enhance availability.

9. In a presentation it was argued that there is a Business Case for security. Customers are willing to pay more if they realise how vulnerable they are. This dimension should be explored further.

10. In this same context, commentators saw a need to assess the economic aspects and cost effectiveness of the ARECI Recommendations. It is important to study the market/economic dimensions of resilient communications.

11. In the current systems, several commentators pointed to the risk brought through the dependency on software-controlled systems and technology. They suggest that the EU promotes systematic vulnerability analysis. It may be useful and provide added value to Member States and private industry to develop at the European level guidelines for systematic vulnerability and robustness testing and the hardening of (existing) software controlled systems

12. Commentators warned for the consequences of the trend of co-location where network operators and providers of applications and services are co-locating, for various reasons. Physical diversity can be compromised; the effect of a single failure has the potential for greater damage. There is a need to study the consequences collocation, co-trenching, duct sharing and the relative openness of the perimeter for personnel from different contractors to co-location sites.

13. It was further suggested that, in order to reduce dependencies of other critical services and supplies and key resources, it must be considered to build firebreaks and/or buffers to stop or slow down a domino effect.

14. Commentators also saw bias in the ARECI report against open source. But they argue open source may offer great benefits to critical infrastructure as it ignores the threats of a software monoculture. They further argue that several critical building blocks are missing from the report when considering the integrity of the supply chain while the report is contradictory in itself. A software monoculture and risk of non-access to source code pose big problems in times of national emergency or crisis.

15. Commentators pointed out the important role of terminal equipment / trusted computing in protecting networks. Linked to this is the ongoing de-perimeterisation in convergent architectures – there is no longer a single perimeter.

16. The mass scale susceptibility of DNS to attack was evoked together with the unwillingness by ISPs / countries to prepare for DNS poisoning.

17. Commentators mentioned the importance of studying and mastering both cross-sector and intra-sector (inter)dependencies as well as the cross-borders operations. In this respect, the focus for EU actions should be on interdependencies and interoperability.

18. The key role of testing / exercising for interoperability, security and crisis management as well as the need to develop Pan-European testing exercises were highlighted.

19. In order to avoid duplication, future actions shall build on and engage existing communities (e.g. FIRST, ISPs etc.).

20. There is a need to deepen the understanding of CIIP issues, in particular with respect to interdependencies. To this end, the importance of well coordinated, structured and interdisciplinary R&D was evoked.

21. Importance of awareness raising towards:→ national/European policy makers
→ intra-sector
→ people (education, schools, etc.)

22. The primary objective of EU actions should be to develop and make available principles to define critical functionality and services as well as good practice guidelines, and not necessarily to develop regulation.

23. There is a need for more pro-active and intelligence based approaches and actions to both resilience and robustness of information infrastructures as well as CIIP.

24. The importance of the "converged" perspective in addressing CIIP was evoked. The "convergence" (at all levels) have changed the horizon and made all networks to be interrelated:
→ not separate infrastructures (IP, service, etc.)
→ not separate networks (fixed, mobile, IP, etc.)

25. The focus of actions on resilience and CIIP should not be on "infrastructures" but on "critical services". What really matters is to ensure business and service provisioning continuity. To this end, "critical services" for business continuity should be defined. By so doing, policy initiatives and actions would primarily focus on benefits and not only on security issues as a whole.

ANNEX 15: REPORT FROM THE SEMINAR ON RAISING SECURITY AWARENESS AND STRENGTHENING THE TRUST OF END-USERS IN INFORMATION SOCIETY

EUROPEAN COMMISSION
Information Society and Media Directorate-General
Audiovisual, Media, Internet
Internet; Network and Information Security

i2010
Information Space
Innovation & Investment in R&D
Inclusion

Brussels, 15.7.2008
INFSO/A3 GG D(2008) 925678 V2.5

High Level Seminar

Raising security awareness and strengthening the trust of end-users in information society: *policy challenges for the next decade*

Brussels, 7 December 2007

Report

1. PURPOSE OF THE SEMINAR

The rise of a ubiquitous information society creates a greater opportunities as well as dependence towards electronic networks and information systems. New forms of organisation, communication, work and living will be possible. Still users should have a feeling of confidence. To address this challenge, the European Commission organised a seminar[1] to discuss which actions should be undertaken to reinforce the trust of the end users in the information society. The discussion took place in the frame of the European Union reflection on the next steps of its strategy for a secure information society[2] within the i2010 initiative[3].

The seminar focus was on the trust of **end users in a broad sense**: citizens, consumers, employees of small or large organisations, and companies themselves as users of ICT products and services.

The seminar elaborated on the statement that confidence can only be achieved if **all stakeholders** directly or indirectly involved in making the information society are aware of their role and of the specific responsibility they should endorse.

The seminar perspective was the information society of the **next decade** where technology will underpin innovative applications like the internet of things but may also lead to new risks (e.g. the consequences of convergence, RFID) as well as provide new countermeasures (e.g. privacy enhancing technologies). The seminar also underlined the possible consequences due to the decisions made today.

The discussion was broad to encompass not only the **technological** evolution but also the **sociological**, **economic** and **legal** contexts.

The seminar gathered **60 persons** representing most of the stakeholders of the security chain: researchers, product manufacturers, system operators, internet service providers, service providers, EU Member States authorities as regulators or service providers, end users represented through a consumer organisation and the Commission (see participants list in annex).

---

1 The terms of reference of the seminar are posted on http://ec.europa.eu/information_society/policy/nis/strategy/activities/awareness_seminar

2 http://ec.europa.eu/information_society/policy/nis/strategy/activities

3 http://ec.europa.eu/information_society/eeurope/i2010

2. FINDINGS

Main findings of the seminar are:

- To achieve high level of network and information security, the participants considered that security should be a concern all along the **development lifecycle** of products and services. It implies **security by design**, rather than afterwards as well as **security by default**. This subsumes the education of developers. Sharing best practices, which should be distinguished from common practice, was also mentioned as an efficient means to increase the security level.
- The topic of **complexity** was raised several times. Increased complexity of networks and information systems is considered as unavoidable. There were some opposite considerations however claiming for promoting simplicity and giving up the trend for increased complexity. Simplicity generally makes security more straightforward. However, security was also seen as the cause of **increased complexity that might hinder user experience and usability**. A challenge for the future resides in designing technologies that are at the same time secure and user friendly: products should be safe by default. In that perspective, it was considered primordial to base research and development of technologies on a **multi-disciplinary** approach, taking in particular user psychology into consideration.
- The **trust in a third party** securing networks and information was claimed to be very relevant to strengthen the trust of users. The trust of users much depends on their confidence that the organisations in charge of processing their personal data or in charge of securing networks will put in place the proper processes and technologies but will not use their power for undue user monitoring.
- The end-user was often pointed as the **weakest link in the security chain** calling for increased efforts from public authorities and the private sector, in awareness raising, education and training. A proposal was made to render IT security mandatory in education curricula. The responsibility of users was also questioned in relation to overcoming what some participants coined as "natural laziness". It was noted that the responsibility of users was limited with regards to technology flaws. However a "baseline" for security could be agreed upon; furthermore according to some participants, each user should have the right to have a secure system and, possibly, each user should even have an obligation to run a secure system. Indeed a non secured system may create risks for third parties. Views however converged in agreeing that **responsibility is shared between all stakeholders**: users, providers of services and products, and public authorities.
- **Economic factors** were also seen as the culprit for a poor level of security deployment as buyers tend to select cheaper rather than secure products. However this argument was countered by stating that there are always users ready to pay for security.
- **Governments** were invited to **lead by showing the example** in investing and deploying secure technologies and putting in place proper processes as a result of conducting continuous risk assessments. The **private sector** and the software industry in particular, should lead on **quality** and security **innovation**.
- The idea of a **legislation requesting minimal level of security** was discussed. Enhanced levels of security could then be a matter of competitive advantage. The challenge resides in defining what should be the baseline. Three potential fields of actions were identified: IT products manufacturing, IT services (adapted according to the application sector) and operation of IT products. Furthermore, participants stressed that if such legislation would be adopted, actual enforceability considerations should be addressed.

- Several participants considered **user empowerment** as crucial. Users should be fully informed of the real risks they are running to make informed security choices. The **asymmetry of information** between users and providers was considered as a key problem. However there were some diverging views stating that security should be transparent to users. In that respect, it was considered wrong to continuously question the user to make security choices which too often actually lead to unsecured situations.
- The problematic of **measuring trust of users** was raised. It is due to a lack of security awareness of probed home users. A main difficulty resides in confronting the perception of trust with respect to the actual risks.
- Finally, the participants agreed that it is too early to have any common reasonable prediction on how security will evolve.

Presentations slides are posted on ec.europa.eu/information_society/policy/nis/strategy/activities/awareness_seminar.

3. CONCLUSION AND WAY FORWARD

The seminar allowed circumstantiating why and how information society actors such as the software producers, access providers, service suppliers, public authorities or users became aware that they have at the same time a role to play and a responsibility to engage. All stakeholders indeed now aspire to the **advent of an ethic**; they wish that the rights and duties of each one are established. That will be possible only if a **new culture of computer security** arises.

In 1762, Jean-Jacques Rousseau wrote about the "*Contrat social*" where each one aspires to "*a form of association which will defend and protect with the whole common force the person and assets of each associate, and in which each, while uniting himself with all, may still obey himself alone, and remain as free as before*"[4]. 250 years later, faced with the complexity of the information society we can be inspired by this spirit to maximise the collective value that brings ICT. To build on the seminar findings, there is thus scope to investigate how such an approach towards a "***Contrat social numérique***[5]**"** could work in practice.

- / -

[4] "*Une forme d'association qui défende et protège de toute la force commune la personne et les biens de chaque associé, et par laquelle chacun s'unissant à tous n'obéisse pourtant qu'à lui-même et reste aussi libre qu'auparavant"*, Jean-Jacques Rousseau, Du contrat social ou principes du droit politique, Livre I, ch. 6, 1762.

[5] "*Digital social contract*" –Thanks to Prof. Michel Riguidel for this formulation.

ANNEX: AGENDA

Introduction of the seminar

- Andrea SERVIDA, Deputy Head of Unit, DG INFSO.A3 Internet; Network & Information Security
- Gérard GALLER, Policy Officer, DG INFSO.A3

Keynote speech: User confidence: where do we stand and where do we go?

- Michel RIGUIDEL, Professor, École Nationale Supérieure des Télécommunications, France

Discussion #1 - TECHNOLOGY

- Janne UUSILEHTO, Head of Product Security, Nokia, Finland
- Olivier PARIDAENS, European Information & Communications Technology Industry Association (EICTA)
- Eilert HANOA, Vice-Chairman of the European Software Association and Founder of Mamut Software, Norway
- Dirk KULHMANN, Research Engineer, HP Laboratories Bristol, Technical Lead of FP6 Integrated Project OpenTC
- George DE MOOR, Professor, University of Gent, Belgium

Debate: Chair and moderator: Dirk van ROOY, Project Officer, DG INFSO.F5 Security

Discussion #2 - DEPENDENCE

- Olivier PARIDAENS, Security Services Business Development Lead, Alcatel-Lucent
- Ferenc SUBA, Chairman of the Board PTA CERT Hungary and Vice President of ENISA's Management Board
- Kurt EINZINGER, Secretary General of ISPA Austria and Vice President of EuroISPA
- Kai RANNENBERG, Professor, Goethe University Frankfurt and coordinator of FIDIS

Debate: Chair and moderator: Andrea Servida

Discussion #3 - PERCEPTION

- Gerald SPINDLER, Professor, University of Göttingen, Germany
- Kornelia KUTTERER, Senior Legal Advisor, BEUC, the European Consumers' Association
- Albena SPASOVA, Director of Law Enforcement Europe, eBay
- Angela SASSE, Professor, University College London, UK
- Tobias HÜSING, Senior Researcher, Empirica, Germany

Debate: Chair and moderator: Anne BUCHER, Head of Unit, DG INFSO.C1 Lisbon Strategy and i2010

Announcement of two related reports by DG Internal Market:

- Fraud Prevention Expert Group (FPEG) report on *identity theft / fraud*, 22.10.2007, http://ec.europa.eu/internal_market/fpeg/index_en.htm
- Final report of a study on *user identification methods in card, e- and m-payments*. Dec. 07, http://ec.europa.eu/internal_market/payments/fraud/index_en.htm#studies
    - Mariano FERNANDEZ SALAS, DG MARKT.F2 Company law, corporate governance and financial crime

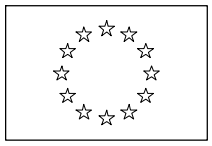
Rapporteur summary

- Christer HAMMARLUND, Policy Officer, DG INFSO.A3

ANNEX: LIST OF THE PARTICIPANTS

Antonio ALCOLEA, Ministry of Industry, Tourism & Trade, Spain
Valérie ANDRIANAVALY, DG INFSO.A3 Internet; Network & Information Security
Ingolf BERG, Ministry of Enterprise, Energy and Communications, Sweden
Charles BROOKSON, ICTSB-NISSG / BERR, UK
Anne BUCHER, DG INFSO.C1 Lisbon Strategy and i2010
Anna BUCHTA, DG INFSO.B1 Policy Development
Gaetan CANTALE, Global Trust Center
Georges DE MOOR, University of Gent, Belgium
Chantal DE VETTE, Ministry of Finance, The Netherlands
Eric DOMAGE, IDC EMEA Software and Services
Kurt EINZINGER, ISPA Austria / EuroISPA
Mathea FAMMELS, ENISA
Mariano FERNANDEZ SALAS, DG MARKT F2 Company law, corporate governance & financial crime
Gérard GALLER, DG INFSO.A3 Internet; Network & Information Security
Oliver GERBER, Swiss Mission to EU
Anta GIANNOPOULOU, Ministry of Economy and Finance, Greece
Gunther GRATHWOHL, Ministry of Economic Affairs, Germany
Christer HAMMARLUND, DG INFSO.A3 Internet; Network & Information Security
Eilert HANOA, European Software Association / Mamut Software
Mari HERRANEN, Ministry of Transport and Communications, Finland
Niels HUIJBREGTS, XS4ALL Internet, The Netherlands
Tobias HÜSING, Empirica, Germany
Achilleas KEMOS, DG INFSO.A3 Internet; Network & Information Security
Victorine KOSSI, DG INFSO.A3 Internet; Network & Information Security
Dirk KUHLMANN, HP Laboratories Bristol / OpenTC Project
Cornelia KUTTERER, BEUC, the European Consumers' Association
Michel LACROIX, DG INFSO.D3 Software & Service Architectures and Infrastructures
Yannis LARIOS, Ministry of Economy and Finance, Greece
Akilles LOUDIERE, Ministry of Economy, Finance and Industry, France
Pierre LUCAS, European Software Association
Eva MARTINICOVA, DG Internal Market E2 Services II
Thomas MYRUP, Microsoft
Radovan PAJNTAR, Ministry of Higher Education, Science and Technology, Slovenia
Olivier PARIDAENS, EICTA / Alcatel-Lucent
Zelimir PECNIK, Central State Administrative Office for e-Croatia
Vlado PRIBOLSAN, CARNet (Croatian Academic and Research Network)
Kai RANNENBERG, Goethe University Frankfurt, Germany / coordinator of FIDIS
Michel RIGUIDEL, École Nationale Supérieure des Télécommunications, France
Martina ROHDE, DG INFSO.A3 Internet; Network & Information Security
Jürgen ROHM, Ministry of Economic Affairs, Germany
Bruno ROUCHOUZE, Eurosmart
Mary RUNDLE, Universities of Oxford, Harvard and Stanford
Horst SAMSEL, Bundesamt für Sicherheit in der Informationstechnik, Germany
Angela SASSE, University College of London, UK
Andrea SERVIDA, DG INFSO.A3 Internet; Network & Information Security
Claire SION, DG INFSO.C1 Lisbon Strategy and i2010
Albena SPASOVA, eBay
Gerald SPINDLER, University of Göttingen, Germany
Eelco STOFBERGEN, GovCert, The Netherlands
Ferenc SUBA, ENISA / PTA CERT Hungary
Luigi TAGLIAPIETRA, CLUSIT, Associazione Italiana per la Sicurezza Informatica
Andreas TEGGE, SAP
Janne UUSILEHTO, Nokia, Finland
Dirk VAN ROOY, DG INFSO.F5 Security
Aniyan VARGHESE, DG INFSO.H2 eGovernment and CIP Operations
Albinas VISOCKAS, Communications Regulatory Authority, Lithuania
Samo ZORC, Ministry of Higher Education, Science and Technology, Slovenia

ANNEX 16: REPORT FROM THE WORKSHOP ON LEARNING FROM LARGE SCALE ATTACKS ON THE INTERNET



EUROPEAN COMMISSION
Information Society and Media Directorate-General

Audiovisual, Media, Internet
Internet; Network and Information Security

REPORT

WORKSHOP ON

LEARNING FROM LARGE SCALE ATTACKS ON THE INTERNET

POLICY IMPLICATIONS

17 January 2008

DISCLAIMER
This report does not necessarily represent the views of the Commission

1. MAIN OUTCOMES OF THE WORKSHOP

On 17.01.08, the European Commission organised a workshop on learning from large scale attacks on the Internet and the policy implications to discuss the lessons learnt and best practices to enhance the security and stability of the Internet. It offered the opportunity to investigate the value of EU and international cooperation as well as Public Private Partnership and it contributed in raising awareness on current Internet security issues.

Lessons learnt: Critical issues to be considered

The discussions have shed light on some of the issues the information society is facing regarding Internet's security and reliability.

The **availability and reliability of Domain Name System** (DNS) services have been identified as two key elements for the correct functioning of the Internet. The **security of traffic exchange between operators** of electronic communications networks and in particular the role of the operators of Internet eXchange Points (IXPs) is an other topic which is currently under the scrutiny of some Member States.

Current trends demonstrate that **malware and attacks are becoming very complex and sophisticated**. Attackers exploit to their own benefit the capabilities of Peer-to-Peer (P2P) networks and, increasingly, the opportunities offered by WEB 2.0. Malware development life cycle is gradually more professionalised. The distribution of malware increasingly follows the commercial practices deployed within the software industry (malware toolkits). Some participants noted that attacks do not exploit anything new however. They take advantage of well known vulnerabilities and make use of existing malicious codes. A speaker mentioned that web pages are increasingly becoming the vector for infections.

Another critical issue is the **asymmetric situation** where attackers are always one step in advance compared to the target. Delegates underlined the importance of better understanding attackers and improving capabilities in monitoring networks under attacks.

Lessons learnt: Current situation

The **distributed nature of the** Internet was recognised as contributing to its flexibility and resilience. Therefore, if related public policies have to be developed, participants argued that they should respect the distributed nature of the Internet and avoid centralisation.

The discussions also demonstrated that the **distributed nature and openness of the Internet participates in its structural vulnerability**. In that respect, the extent of electronic communications infrastructures was questioned as the computers of end-users (i.e. at the edges) may increasingly be considered as part of the global infrastructure. The distributed nature of P2P is more and more exploited to decentralise the command of malware. As a consequence, attackers are hard if not impossible to identify and deter.

Participants converged in recognising that the **Internet's security and stability is a shared responsibility**. Every stakeholder (public authorities, the private sector and individuals) has a role and responsibility. In that respect, delegates pointed out that the level of security put in place by one entity might eventually brings more benefits to others. This paradox raises the question which incentives should be brought forward to stakeholders to adopt security measures.

Lessons learnt: The way forward

Several participants underlined the crucial necessity to **build further the resilience and robustness of the Internet**. One of the directions proposed was related to ensuring the redundancy of servers and connections. In particular the deployment of Anycast technology was considered valuable to ensure the resilience of DNS services. The value of diversity in the strategies and operations in order to avoid single points of failure, and consequently making it harder for attackers to succeed, was highlighted. The security of routing protocol and traffic exchange would also deserve further attention. Concerning the reliability of DNS services, a delegate mentioned that the deployment of DNS Security Extensions (DNSSEC) has been put into operation in his country.

With regard to malicious activities, the adage "***know your enemies***" was brought to the table by participants who mentioned that behavioural analysis and attackers profiling were key. Delegates pointed out the value and limit of tracking compromised machines. Isolating a country or an organisation to avoid the impact of malicious activities originating from outside the borders was considered unfruitful while amplifying the success of an attack.

At the same time, several participants stressed that **response preparedness is crucial**. The directions mentioned revolve around national contingency plans for the Internet, regular cyber exercises on national/international level and the strengthening of multinational cooperation for rapid response (in a formal rather than informal basis). The importance of building incident response capabilities which could be supported by Computer Emergency Response Teams (CERT), also called Computer Security Incident Response Teams (CSIRT), and their role for national and international cooperation was underlined.

In order to get a better picture of networks' availability and resilience, it is more and more essential to **measure and monitor network traffic**. A "*collective intelligence approach*" was called upon: computers of end users could be leveraged to gather and process the necessary data. Efforts on strengthening early warning systems were considered as crucial to reduce response time and damages. At the same time, the increasing large amount of security information that needs to be analysed is a challenge.

Participants recognised that the **technology will not be sufficient** to reach the adequate level of Internet's security and stability. They highlighted the importance of other aspects:

- Setting-up **Public Private Partnership (PPP)** to build further the resilience of the Internet, prepare the response and improve the understanding of the situation. The role of governments is to coordinate and be a good user;

- Developing cross-sector and cross-organisational **cooperation** at national, European Union (EU) and international levels as well as agreeing on **responsibility's allocation** along the value chain;

- Promoting **information and best practices sharing** for which trust is a precondition; a (legal) framework that permits information sharing was deemed necessary;

- Raising **security awareness and education** of individuals, public bodies, corporate users and service providers;

- Understanding the economics of security and cyber crime.

Eventually, the discussions demonstrated that there is a crucial need to **bridge the gap between policy makers and the technical community**.

2. CONTEXT

The European Commission announced in its Commission Legislative Work Programme for 2008[226] the intention to adopt a policy initiative on critical communication and information infrastructures protection (CIIP), under the broader framework of the European Programme on Critical Infrastructure Protection[227]. The objective of this initiative will be to ensure that adequate and consistent levels of **preventive, detection, emergency preparedness and recovery measures** are in place across the EU.

The workshop fostered the discussion on 1) the lessons-learnt from large scales attacks on the Internet and on 2) the best practices devised by stakeholders to enhance the security and stability of the Internet. It offered the opportunity to discuss and investigate the value of EU and International cooperation as well as Public Private Partnership. It also contributed in raising awareness of participants on current Internet security issues.

The workshop gathered 86 participants from Member States bodies, academia, industry and European institutions. The 57 delegates from 21 EU Member States, plus Norway, represented the ministries of defence, interior affairs, industry, communications, finance, or telecom National Regulatory Authorities. Twelve security experts from academia and industry attended the meeting.

The workshop followed the subsequent structure:

(1) A first session on **setting the scene on recent large scale attacks**. This session is reported in chapter 3.1;

(2) A track dedicated to **lessons learnt in terms of preventive measures** to mitigate the risks beforehand. This session is reported in chapter 3.2;

(3) A session on **lessons learnt in terms of detection and response capabilities** to improve preparedness in detecting and responding to incidents. This session is reported in chapter 3.3;

(4) A track on **horizontal measures**. The session focused on the measures to identify and map stakeholders' roles and responsibilities. This activity is horizontal to the measures aiming to improve prevention, detection and response capabilities This session is reported in chapter 3.4;

(5) A final session on **the way forward** summarised the outcomes of the workshop. This session is reported in chapter 1 which records the main outcomes of the workshop.

[226] See Commission communication - Commission Legislative and Work Programme 2008, COM(2007)640 of 23.10.2007

[227] See COM(2006) 786 of 12.12.2006 and COM(2006) 787 of 12.12.2006

3. REPORT ON THE SESSIONS

This chapter presents the views expressed by the participants in the sessions on setting the scene, lessons learnt in terms of preventive measures, detection and response capabilities and the session dealing with horizontal measures.

3.1. Setting the scene on recent large scale attacks

This session provided an overview of large scale attacks on the Internet from three different perspectives: the coordinated cyber attacks against the Internet resources of Estonia, the attacks targeting DNS root servers in 2002 and in early 2007 and the trends in malware propagation.

One of the lessons learnt from the coordinated cyber attacks against the Internet resources of Estonia has been that Network and Information Security is all about trust built on a joint effort. Among other things, the new Estonian cyber security strategy highlights the importance of improving interdepartmental coordination mechanisms for rapid response and recovery. Setting-up incident response capabilities and in particular Computer Emergency Response Teams (CERTs) and developing a cooperation model among them is also crucial to face coordinated attacks. The role ENISA is playing in supporting the coordination between CERTs has been recognised as instrumental.

DNS is another important element of the Internet[228]. Concerning the attacks to the DNS root servers in October 2002 and February 2007[229], they were actually attacks to the network infrastructure and not to the service itself. It was reported that the DNS services were actually never down. The attacks have demonstrated that it is rather the infrastructure connecting the DNS servers that is vulnerable. It was pointed out nevertheless that the best service is useless if you cannot reach it because the infrastructure is down. Thus, an improvement in the system's infrastructure is needed; in particular, more servers are required to ensure that the services can be reached. The DNS service itself is considered as very resilient by design. Also, with respect to the attack in October 2002, there was no clear picture of the actual damage. To cope with this lack of perception, RIPE developed a better distributed measurement system to assess the availability of DNS service.

Regarding malicious activities on the Internet, one of the speakers pointed out the following trends:

- Attackers are getting more and more professional and sophisticated. The distribution of malware increasingly follows the commercial practices deployed within the software industry via malware toolkits;
- Large botnets have between identified to host 250 000 to 1 million zombie machines. They are mainly used to send spam but also for Distributed Denial of Service attacks;
- Malware functioning is changing from a central command and control architecture to a peer-to-peer architecture;
- The web is increasingly the vector for infections;

[228] DNS services underpin the resolution of domain names (for instance www.example.com) into IP addresses which are used by computers to communicate over the Internet.

[229] See ICANN fact sheet at http://www.icann.org/announcements/factsheet-dns-attack-08mar07_v1.1.pdf

- The number of malware is booming. There is an increasing trend in the number of bots and Trojan horses and a decreasing one in the number of viruses and worms. The anti-malware industry was reported as facing difficulties to keep up with the overload of malwares;

- The effectiveness of anti virus is unfortunately reducing and a new strategy should be considered. A speaker mentioned that a study has evaluated that approximately 40% of analysed computers have updated anti-viruses installed and, up to 15 to 20% of the computers with updated anti-viruses protection might be infected with active malware;

- We should not forget that there is also an increasingly large number of small scale attacks occurring (not just large scale ones).

The speakers and the participants proposed some directions to be followed. Better technology approaches based on collaborative intelligence and behavioural analysis should be considered. With a collective intelligence approach it would be possible to correlate data, through different sensors installed on the network, responsible for collecting data and sending it to a machine to process it. Computers at the edges could be leveraged to build this collective intelligence.

Behavioural analysis and profiling attackers is essential to understand attackers' motivations and consequently better protect the infrastructure. It was reported that a Europol working group is working on profiling cyber attackers.

At the same time, it would be needed to foster cooperation between jurisdictions. In particular, Internet Service Providers (ISP) should be able to share information in order to be able to respond effectively. The help of domain registrars would also be valuable to report on rapid changes of domain information. Moreover, the importance of the existence of multinational rapid response teams cooperating on a formal rather than informal basis was highlighted.

Encouraging the hardening of networks was also considered as a necessary step to enhance Internet's resilience. Proposed technical solutions included the deployment of Anycast and ensuring redundancy of servers and connections. Participants pointed out, however, that the motivation for hardening the networks could be impaired by the fact that, sometime, the hardening brings more value to others than to the one putting it in place; the benefits might not be local but remote. Therefore, it is important to involve all stakeholders in making an effort to contribute to the same objective, possibly through public-private partnerships.

In addition, participants have put forward several policy options to be considered in mitigating attacks. Firstly, take advantage of the technology and implement measures at ISP level to decrease malicious traffic. Secondly, implement better domain registration controls to impede malicious activities. Finally, extend regular vulnerability scans to all businesses with web sites.

It was also mentioned that the Internet is not a self-organising and self-fixing network as theoretically portrayed. The distributed nature of the Internet should be hailed for the role it plays in contributing to more flexibility and resilience. Therefore, if related public policies have to be developed, participants commented that they should respect the distributed nature of the Internet. Plans for centralisation should be avoided.

3.2. Lessons learnt in terms of preventive measures

The session first dealt with measures to enhance the robustness of the infrastructure underlying the Internet (DNS security, redundancy of links, etc). The second part covered measures to enhance the security of servers which host the web sites composing the Internet.

Development and deployment of measures to protect Internet infrastructure

The Swedish experience in building a strategy to improve Internet security was presented. As preventive measures, Sweden focused on building rock shelters for ISP equipment as well as extra redundancy in network infrastructure (with the financial support of the government) and ensuring cooperation between telecom and electricity suppliers. The later 2006 government's strategy for a more robust and resilient Internet infrastructure has put forward preventive measures that include the following: a recommendation for providers of services to increase website accessibility, a new law to ensure better management of the national Top-Level Domain, the promotion of Domain Name System Security Extensions (DNSSEC) deployment and use, the improvement of security at the traffic exchange points between ISPs, the creation of a contingency plan for the Internet and the establishment of a National Crisis Management Group. The success of public-private partnerships in the development and implementation of better crisis management and in facilitating actions for security and robustness was pointed out.

While the current level of availability of the DNS service was considered as becoming less problematic, the lack of reliability of the DNS responses was pointed out in contrast. It was questioned whether DNSSEC could help improving the situation by ensuring that the responses from the DNS server can be trustworthy through digital signatures. Concerning availability, more geographical distribution should be promoted. Anycast is a proven technical solution that might help building redundancy. Having an Anycast server closer to the source of attack (from a network topology perspective) will attract the "bad" traffic of an attack and therefore its global impact will be reduced. In the same way, being able to resolve all the world's domain names at a local level reduces the opportunity for attacks on DNS global infrastructure. Service providers should also use and deploy multiple platforms (software and hardware), from different sources, to reduce exposure. A key principle is to avoid single points of failure.

The Border Gateway Protocol (BGP) was also considered insecure entailing the risk of generating false routes at Internet eXchange Points (IXP). Attention was drawn to safeguard the routing between ISPs. To this end, Internet eXchange Points operators should build efforts to offer greater peering capabilities through stable and resilient peering platforms.

Views on how to protect Internet infrastructure have identified the importance of staying ahead of crime through ongoing infrastructure investment, continuous monitoring and analysis of traffic trends. Multiple platforms should be deployed in multiple locations. Early warning should be based on information sharing to identify likely types of attacks. It was also remarked the value of diversity in the strategies and operations in order to avoid single points of failure, and making it harder for attackers to succeed. In this context, isolating a national network that is under attack does not help mitigating the problem, but rather increases the chances of attackers to achieve their objectives. Moreover, there was also the view that as long as cyber-crime is a driver, then the infrastructure is normally safe, because its integrity and availability is also needed to perpetrate attacks.

Conducting and learning from international exercises were also considered as vital to ensure preparedness and better response in the event of attacks.

Measures to protect the provision of web services

The approach of CERTA, the French CSIRT, in improving Internet security was presented. CERTA prevents and deals with security incidents, and informs and trains citizens about trends and vulnerabilities. It also promotes real-case scenario exercises involving ministries and contributes to end-users education.

Participants highlighted the role of security intelligence in becoming pro-active towards security. An example of a large global intelligence network was presented. The network is composed, among other elements, by 40 000 registered sensors in more than 180 countries, 8 security responses centres distributed around the globe and it monitors 30 % of world's e-mail traffic.

Security firms report that attacks are getting more and more sophisticated. In the last six months most of the attacks used malware toolkits like MPack. In fact, most of the massive attacks are not using anything new, but well known vulnerabilities and malicious codes. The vulnerabilities of Web 2.0 are also more and more exploited. It was remarked that underlying web applications are not always receiving the same level of security auditing as traditional client-based applications.

Conclusions about measures to protect web services suggested the following:

- Both large and small providers should uniformly adopt security measures;
- Service providers should follow standards. The adoption and compliance to ISO/IEC 27001 and ISO/IEC 27002 should be promoted;
- Software best practices and robust services are needed;
- The role of security intelligence is crucial to become pro-active;
- National and International cooperation is key. In that respect the importance of CERTs and National Centers for the Protection of the Critical Infrastructure was underlined;
- Re-enforcing cooperation within a clear legal framework between law enforcement authorities, governmental CERTs and the private sector is needed;

Once again, the distributed nature of the Internet and the high dependency chain involved, as well as, the shared and distributed responsibility towards the Internet were pointed out. In the case of public-private partnerships, governments should not only play a role of coordinators but also of good users. Trust between stakeholders is crucial especially when it comes to cooperation.

The importance of learning from the experience of the financial sector, which is suffering hundreds if not thousands of targeted attacks a day, was also pointed out.

Eventually, it was questioned again which incentives should be brought forward to stakeholders to adopt security measures considering that the level of security put in place by one entity is not strictly local but would eventually bring benefits to the others.

3.3. Lessons learnt in terms of detection and response capabilities

The session first dealt with large scale detection systems and early warning systems that can be used to support national and European strategies. The second part dealt with procedures and mechanisms to structure response activities and damage limitation across Member States.

Detection and early warning and alert systems

Having an early warning system in place to be able to respond faster and to control the damage is crucial. The main objectives of such early warning system should be, *inter alia*, to improve the scope of detection capabilities through the installation of more probes in the network, improve response time in order to reduce the impact of attacks, and strengthen international cooperation.

The Dutch experience suggested that combining efforts with other CERTs to set up a Pan-European early warning system ("*Pan-European dashboard*") could be of great interest.

It was also reinforced the need for more and better collaboration between stakeholders and the need to extend it to an international level, as it is assumed that large scale attacks will tend to always have an international component. Collaboration today is mainly based on the efforts of ENISA, EGC (European Government CERTs), TFCSIRT (Terena's taskforce to promote collaboration between European CERTs), FIRST (international forum of CERTS) and on ad-hoc relationships.

Thus, a trusted and reliable international network, based on formalised collaboration and information sharing, was called for. The overall strength could be built on each CERT unique qualities. A complete and reliable network of contacts in Member States would facilitate the task. It was noted however that not all countries foresee to have central contacts. It was also requested more support and funding for CERTs to fight cyber crime while nowadays this type of funding is mainly directed to intelligence and police. A definition of which CERT capabilities could be attributed to European Community agencies should be decided. For what concerns information sharing, the attention was drawn on the creation of technical and legal mechanisms to encourage and help organisations to share and exchange attack-related data and to put in place a legal framework for data sharing that clearly defines who, when and for which purpose can data be accessed.

Readiness to react to attacks relayed by large number of distributed sources

In this session, the lessons learnt from the large scale attacks against Hungarian banks and Estonia's Internet resources were presented.

A few years ago seven Hungarian banks were the target of a large scale phishing attack executed by international botnets during two weeks. Stakeholders involved in mitigating the problem included the banks, national and international CERTs, ISPs and law enforcement agencies. The lessons retained from these attacks are the importance and need for enhanced level of preparedness, early warning, manpower, coordination, involvement with international partners and media work.

The Estonian attack was conducted by circa 4000 compromised machines and affected the country's infrastructure. Compared to other large scale attacks, the Estonian incident was relatively small, but it was just right for the scalability of the national infrastructure, resulting in a considerable impact. Stakeholders involved in the incident response consisted of CERTs (the Estonian one as well as experts from the international CERT community)

and ISPs. Lessons learnt from this attack revealed the importance of fast incident response capability and of CERT organisations and, most of all, the cooperation/communication between them. The global extent of the Internet also calls for international cooperation and international contingency plans.

Recommendations to tackle large scale attacks from distributed sources put forward by participants comprised the following:

- Foster dialogue for policy making, e.g. by a EU Platform for ISPs, owners of Critical Infrastructures, governments and CERTs;
- Recommend a model for EU operational coordination based on best practices, in the financial sector and in particular via Information Sharing and Analysis Centres Councils;
- Promote European exercises involving large industry players, Member States and EU agencies on a voluntary basis;
- Support voluntary cooperation between Member States' early warning systems;
- Redefinition of critical infrastructure to include private and business infrastructures, considering the impact of personal computers in this type of attacks;
- Have contingency plans to maintain the Internet within the country and survive without the outside Internet;
- Facilitate law enforcement cooperation globally.

3.4. Horizontal measures

This session covered the identification and mapping of stakeholders' roles and responsibilities. This topic is horizontal to measures aiming to enhance the prevention, detection and response capabilities.

The German Implementation Plan for Critical Infrastructure Protection (CIP) was introduced. The main ideas that have been put forward in the plan revolve around recognising that the security of critical infrastructures is a joint responsibility, trust is crucial and cross-sector and public-private collaboration is necessary. This implementation plan has been drafted in cooperation between a large number of critical infrastructure operators and public administrations. It is based on the need to address protection of information infrastructures, preparedness in response to IT (Information Technology) incidents and sustainability, in particular, in ensuring IT competence. The role of the government in defining the CIP strategy and in operating a situation room and analysis centre, as well as, the role of the operators/owners of critical infrastructures in implementing the strategy and the recommendations proposed in the CIP Implementation Plan were underlined.

ccTLD (country-code Top Level Domains) registries should invest in systems resilience to ensure the security and resilience of the Internet. Systems resilience is built via correct dimensioning, connectivity and redundancy, rather than in improving the DNS system itself, as the latter is supposed to be resilient in its design by providing caching and redundancy.

For what concerns the role of ISPs, it was pointed out that the word ISP encompasses a wide range of actors, i.e., access providers, hosting providers, email service providers, online service providers, etc. ISPs aim for self-regulation. For instance, business continuity plans should be internally developed in order to deliver the capability of reacting rapidly to unexpected and unpredictable attacks. It is also desirable to have comprehensible legislation and regulation in place. In that respect, bridging the gap between policy makers and the technical community is crucial.

As a conclusion all participants reiterated that IT security is a shared responsibility and can only be guaranteed if all stakeholders accept their responsibilities and build up mutual trust and understanding. Another important component is national cooperation between all the stakeholders. Cooperation needs to be extended to an international level too, as the global character of the Internet does not permit one country isolating itself from the Internet.