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 1)

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

TABLE OF CONTENTS

TABLE OF ANNEXES

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Organisation and timing

Annex 1 contains a detailed table depicting the timetable of the consultation of interested parties, of the meetings of the inter-service steering group and of the Impact Assessment report itself.

1.2. Consultation and expertise

During the preparation of this initiative, **DG INFSO sought the involvement of all relevant stakeholders**. Within the Commission, an Inter-service Steering Group was set up. The following services participated in the group: DG JLS, DG TREN, DG ENTR, DG MARKT, DG COMP, DG SANCO, DG ENV, DG EMPL, DG DIGIT, DG RELEX, DG SJ and DG SG.

The Inter-service Steering Group met three times. The kick-off meeting took place on 14 December 2007, when DG INFSO presented the initiative and the planned work to be carried out. A second meeting was organised on 20 October 2008, for the presentation of the draft final report of the external study on the assessment of the impacts of the possible policy options and a preliminary discussion on the work on the impact assessment report itself. During the third meeting, organised on 4 November 2008, the draft final impact assessment report was discussed.

The different aspects of this policy initiative have been discussed as widely as possible following an inclusive approach and respecting the principles of participation, openness, accountability, effectiveness and coherence. The milestones of this consultation process, which started in 2007, were:

- **18th January 2007** – public forum on the availability and robustness of electronic communication networks[1].
- **19th January 2007** - further to the study on the "Availability and Robustness of Electronic Communication Infrastructures" (ARECI)[2] conducted by Alcatel-Lucent, the Commission invited comments on the study's recommendations and held an informal meeting with Member States' experts.
- **2nd April 2007 – 18th May 2007** – public consultation on the final report edited by ALCATEL-LUCENT on the study on "Availability and Robustness of Electronic Communication Infrastructures" (ARECI)[3].
- **18th June 2007** - second meeting with Member States and industry representatives to discuss how to enhance the availability and robustness of electronic communication infrastructures [4].
- **19th September 2007** – workshop on business continuity plans of country-code Top Level Domains (ccTLDs) DNS operators. A detailed report of the workshop has been prepared by DG INFSO.
- **31st September 2007** - public consultation on an EU Strategy for International Co-operation on ICT (section 4.1 contains a question on the role of the European Commission in developing global cooperation on CIIP)[5].
- **7th December 2007** - Seminar on raising security awareness and strengthening the trust of end-users in information society[6].
- **17th January 2008** - Workshop on lessons learnt from large scale attacks on the Internet and relevant policy implications with delegates from Member States and representatives from

1 See http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3141.

2 See http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm.

3 See http://ec.europa.eu/information_society/policy/nis/docs/studies/areci_study/Report_ARECI_Consultation_Summary_final.pdf and Annex 13.

4 See http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm and Annex 14.

5 See http://ec.europa.eu/information_society/activities/internationalrel/global_issues/consultation/index_en.htm.

6 See http://ec.europa.eu/information_society/policy/nis/strategy/activities/awareness_seminar/index_en.htm and Annex 15.

organisations involved in the protection of critical communications and information infrastructures, in order to identify key priorities and elements for actions at EU level.[7]

- **5th February 2008** – First meeting with Member States on the process to define sectoral criteria to identify European Critical Infrastructures in the ICT sector. A subsequent meeting was held on 29th May 2008. A Staff Working Paper has been circulated for comments between Member States' experts on 30 May 2008.
- **12 February 2008** – A questionnaire has been sent to Member States to take stock of national CIIP initiatives and processes to define ICT criteria. A Staff Working Paper analysing the result of the questionnaire on the national CIIP initiatives was circulated for comments between Member States' experts in October 2008[8].
- **26th June 2008** - Meeting with private sector representatives was held on the role of the industry in the context of CIIP.

The consultation process involved a wide variety of stakeholders and experts which played an important role in the development of the policy proposal. These include representatives of:

- **Member States' public bodies** involved in enhancing the level of network and information security and/or the protection of Critical Communication and Information Infrastructures;
- **national public bodies and National Regulatory Authorities** in charge of regulating electronic communications networks and services;
- **electronic communications operators**, **Internet Service Providers**, and related sector associations (e.g. ETNO, ECTA, EuroISPA, EuroIX, etc.);
- **other Internet operators** (e.g. ccTLD registries, RIPE, Community DNS);
- **suppliers of hardware and software components** for electronic communications networks and services, and related sector associations (e.g. BSA, ESA);
- **providers of products and services for Network and Information Security**;
- **other organisations** involved in the field of network and information security such as CERTs,[9] the Joint Research Centre (JRC), ENISA.

1.3. Opinion of the Impact Assessment Board

The Commission's Impact Assessment Board (IAB) was consulted on the draft final Impact Assessment report and issued its opinion on 18 December 2008. The IAB considered that "substantial preparatory work has been carried out and a good use of summary tables and boxes is made". The IAB also formulated a number of recommendations, which have been duly addressed in the final report. The baseline scenario has been developed further by adding all related EU level initiatives and policy proposals already proposed by the Commission. Additional details have been provided to demonstrate better the added value of further EU action (Section 2.3). The recommendation to elaborate more on the international risks has been taken up in Section 2.1.4. Section 6 has been redrafted in order to further substantiate that non-binding measures would be in all respect more effective than binding measures. The table of impacts has been modified so that the different policy options are assessed as net changes relative to the baseline (Annexes 3 and 4). In addition, a summary table of the main impacts has been added to the main text. In view of improving the presentation of the report, essential elements of the information contained in the annexes have been presented in the main part of the report, keeping into account the length limitations and the fact that the annexes constitute an essential part of the overall Impact Assessment.

---

7 See http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/index_en.htm and Annex 16.

8 See Annex 17.

9 See section 2.1.7.

2. PROBLEM DEFINITION

2.1. What is the issue or problem that may require action?

Information and Communication Technologies (ICTs) have become the backbone of the EU economy and society as a whole. **The ICT sector is vital for all segments of society**: for the private sector, for governments and public administrations and for the citizens. **Businesses rely on the ICT sector** both in terms of direct sales and of the efficiency and effectiveness of internal management and production processes. ICTs are also **more and more pervasive for the functioning of governments and public administrations**: the uptake of eGovernment services at all levels, while guaranteeing more efficient decision-making and administrative procedures, makes the whole public sector heavily dependent on ICTs even for basic operations. Last but not least, **citizens increasingly rely on Information Society services and use ICTs in their daily activities.**

ICT systems and services are a vital infrastructure *per se* as well as an underpinning platform for other critical technological and societal infrastructures. This criticality was acknowledged in the European Commission Green Paper on a European Programme for Critical Infrastructure Protection which captured with the concept of **Critical Information Infrastructures (CII)** all "*ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)*"[10]. A similar definition was also proposed by OECD: "*those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy*"[11]. Despite the existing differences on how the CII is understood in different national and international policy contexts, **what is important is that the notion of CII is conducive to a more holistic policy perspective for the secure and continuous functioning of ICT systems, services, networks and infrastructures** (**ICT infrastructures**) of which the **Internet is a very important component**, due to its widespread diffusion and the process of technological convergence.

Many services and processes have become increasingly dependent on the well functioning of CII, which contribute to wealth creation and ensure the maintenance of vital societal functions, including health, safety, security, economic and social well-being of EU citizens. Moreover, **CII are needed to support the work of other critical infrastructures, from energy distribution and water supply to transport, finance and other critical services**. As a consequence, the failure of a single network or information system could have a huge effect per se and, in addition, potentially propagate widely, possibly beyond national borders, and affect other sectors. **Enhancing the security and resilience of CII has to be a top priority as it provides the frontline of defence** against failures and attacks, in addition to the necessary measures aimed at preventing, fighting and prosecuting criminal and terrorist activities targeting CII.

2.1.1. The economic dimension

The ICT sector is becoming more and more important for European economy and society, as evidenced by various survey data. It is a critical component of innovation and is responsible for nearly 40% of productivity growth[12].

More and more Europeans live in a truly information-based society where the use of ICTs has rapidly increased to become a core function of human social and economic interaction. According to Eurostat, 93% of EU enterprises and 51% of citizens **actively used the Internet in 2007**, with the number of regular Internet users having increased by 40 million in just one year.[13]

---

10 See COM(2005) 576 final, Green Paper on a European Programme for Critical Infrastructure Protection, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF.

11 See the OECD Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35] at http://www.oecd.org/dataoecd/1/13/40825404.pdf.

12 Eurostat, Theme: Science and Technology/Information Society, http://epp.eurostat.ec.europa.eu.

13 Eurostat, Theme: Science and Technology/Information Society, http://epp.eurostat.ec.europa.eu.

Mobile penetration rates have risen to 112% in 2007, compared to 103% in 2006. 3rd Generation (3G) mobile penetration doubled to 20% in 2007, now representing over 88 million subscriptions, and in parallel, mobile data services grew by around 40%.[14] **The number of fixed lines is also very high – for 2006 it was 47 per 100 inhabitants**.[15]

Connectivity and basic ICT uptake have visibly progressed in the last years and high-speed broadband connection is becoming the norm. With 100 million broadband Internet connections, the European broadband market is growing rapidly and is now larger than the one of the United States. **By January 2008, 77% of all businesses had a broadband connection**.[16] **Eurostat reported in 2007 that 42% of households had a broadband connection**.[17]

Internet take-up led to an ever increasing use of various services supported by ICT infrastructures. According to Eurostat[18], in 2007, the value of purchases and sales by Internet and/or networks other than Internet amounted to 11% of total turnover of EU enterprises. In addition, it is estimated[19] that in the period 2007-2010 the online sales will almost double for Western European countries, whereas for CEE countries the increase will be more than two times, reaching a total of 261.3 billion EUR. In 2007, 77% of businesses were using the Internet for their interaction with banks.[20] In addition, **enterprises and individuals started making significant use of e-government services**,[21] stimulated by progress in the availability and sophistication of online public services. In 2007, **30% of individual Internet users interacted online with public authorities, and the figure for businesses is more than 65%**.[22]

Other online services, such as eHealth[23] are gaining importance. In 2006, no less than 40% of adults in Finland, Iceland and the Netherlands relied on the web for information about health, as did over 30% in Norway and Germany, to identify symptoms, understand their prescriptions, and so on.

There is every reason to think that in the future, ICT will continue to reach further into the daily lives of citizens and businesses.[24]

2.1.2. The increasing reliance on pervasive ICTs

In parallel with the development towards increased utilisation and dependency on information infrastructures**, there is a rapid technological development of ICT infrastructures**. The result is a flow of new and more advanced services. At the same time, **ICT infrastructures are becoming increasingly complex and exposed to more rapid changes than before**. The number and nature of devices accessing communication networks have multiplied including fixed, wireless and mobile devices. Also, a growing percentage of access is through "always on" connections. Consequently, **the nature, volume, importance and sensitivity of information that is exchanged have expanded substantially**.

Moreover, ICT infrastructures are fundamentally peculiar, as they **play the crucial and twofold role of being both critical infrastructures themselves and an essential enabler for other critical infrastructures**, which rely on them for monitoring and control – increasingly feasible from remote locations, possibly via publicly accessible networks. The existing interdependencies between different sectors create a situation where a particular event may have a cascading effect

14 COM(2008) 153 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions – Progress Report on the Single European Electronic Communications Market 2007.

15 Eurostat, Theme: Science and Technology/Information Society, http://epp.eurostat.ec.europa.eu/.

16 97% of large enterprises and 77% of SMEs – see http://ec.europa.eu/information_society/eeurope/i2010/infso_today/index_en.htm.

17 Eurostat, Theme: Science and Technology/Information Society, http://epp.eurostat.ec.europa.eu/.

18 Eurostat, Theme: Science and Technology/Information Society Statistics/ E-Commerce by individuals and enterprises/ Value of purchases and sales by Internet and/or networks other than Internet.

19 DigiWorld Yearbook 2008, The Digital World's Challenges

20 http://ec.europa.eu/information_society/eeurope/i2010/mid_term_review_2008/index_en.htm.

21 http://ec.europa.eu/information_society/activities/egovernment/index_en.htm.

22 Eurostat, Theme: Science and Technology/Information Society

23 http://ec.europa.eu/information_society/activities/health/index_en.htm.

24 Susanne Huttner, "The Internet economy: Towards a better future", available at www.oecdobserver.org/news/fullstory.php/aid/2330/The_Internet_economy:_Towards_a_better_future_.html.

on other sectors and areas of life, which are not immediately and obviously interconnected.[25] As a consequence, in our modern technological society, infrastructures and systems become more fragile and may fail faster than ever before, because of a major accidental technological failure of or an attack to a communication or information network. In addition, the risks due to man-made attacks (whether intentional or accidental), natural disasters or technical failures are often not fully understood and/or sufficiently analysed. As a consequence, the level of awareness and understanding across stakeholders is not sufficient to allow the definition and implementation of adequate and effective safeguards and countermeasures.

This calls both for a greater awareness of the risks to ICT infrastructures as well as for a risk management approach to tackle risks and provide adequate tools to manage them.[26]

2.1.3. The potential cost of cyber-attacks and cyber-disruptions

The vulnerability of CII exposes society to high economic cost once incidents occur. For example, the World Economic Forum estimated in 2008 that **there is a 10 to 20% probability of a major CII breakdown in the next 10 years, with a potential global economic cost of approximately $250 billion**.[27] Research conducted for Business Roundtable by Keybridge Associates[28] suggests that **the economic costs of a month-long Internet disruption to the United States alone could be more than $200 billion**. A UK payment association estimated that the direct losses caused by malware to its member organisations grew from £12.2 million in 2004 to £33.5 million in 2006[29]. According to the UK information security breaches survey[30], the worst security incidents caused disruption of service to small businesses for 1-2 days at an average cost of £8,000-£15,000 each, whereas large businesses suffered average interruptions of 1-2 days at an average cost of £80,000-£130,000 each. The average total cost of the worst incident (including direct financial cost and reputation damage) for large business is £90,000-£170,000 and for very large business is £1-£2 million.

There are different threats to CII, such as natural hazards (floods, earthquakes, volcanic eruptions, etc.), failures and accidents (hardware failures, software bugs, involuntary human actions such as errors or omissions, etc.), events caused by voluntary human actions (theft, industrial sabotage, cyber-crime, terrorism or political motivations). **Recent years have seen a growing use of cyber-attacks** (i.e. attacks to, and often using, ICT infrastructures) **for a variety of purposes**.[31]

---

25 Some non-exhaustive examples: in January 2003, the "Slammer" worm, which caused major problems for IT systems around the world, penetrated the safety monitoring system at a US nuclear plant for nearly five hours. The US Nuclear Regulatory Commission investigated the incident and found that a contractor established an unprotected computer connection to its corporate network, through which the worm successfully infected the monitoring system of the nuclear plant. More recently, the United States indicted James Brewer for operating a botnet of over 10,000 computers across the world, including computers located at Cook County Bureau of Health Services (CCBHS). The malware caused the infected computers to, among other things, repeatedly freeze or reboot without notice, thereby causing significant delays in the provision of medical services and access to data by CCBHS staff. See OECD, Malicious Software (Malware): A Security Threat to the Internet Economy, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL.

26 See Annex G to the 2008 OECD Seoul Declaration on the Future of the Internet Economy, where a risk management approach to CII is explicitly called for, with measures aimed at "[d]eveloping a national strategy that gains commitment from all those concerned, including the highest levels of government and the private sector. Taking into consideration interdependencies. Conducting a risk assessment based on the analysis of vulnerabilities and the threats to the CII, in order to protect economies and societies against the impacts of highest national concern. Developing, on the basis of the assessment, and periodically reviewing a national risk management process that sets out the detailed organisation, tools and monitoring mechanisms required to implement the risk management strategy at every level".

27 See World Economic Forum, Global Risks 2008 – A Global Risk Network Report, 2008, available at http://www.weforum.org/pdf/globalrisk/report2008.pdf.

28 Business Roundtable, Growing Business Dependence on the Internet, 2007.

29 APACS, http://www.oecd.org/dataoecd/33/53/38652807.pdf

30 BERR, Information Security Breaches Survey 2008.

31 It should be noted that both the DDoS attacks that targeted Estonia in 2007 (see annexes 7 and 16, as well as Gadi Evron, Battling Botnets and Online Mobs – Estonia's Defense Efforts during the Internet War, Georgetown Journal of International Affairs, Winter Spring 2008, available at http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf, and SEMA, Large scale Internet attacks – The Internet attacks on Estonia – Sweden's emergency preparedness for Internet attacks, 2008, available at http://www.krisberedskapsmyndigheten.se/upload/3040/Large%20scale%20Internet%20attacks_utb-ser_2008-2.pdf) and the "web defacement" attacks which in 2008 targeted Lithuania (see annex 18 A) were attributed, at least partly, to political motives. More specifically, it has been suggested that one of the underlying drivers of the attacks were respectively the decisions by the Estonian parliament to relocate a monument dedicated to the memory of Soviet soldiers and of the Lithuanian parliament to ban the display of Soviet-era symbols, as well as the playing of the Soviet national anthem, therefore prompting the action of pro-Russian individuals and groups.

Moreover, **cyber-attacks have risen to an unprecedented level of sophistication**. What used to be simple experiments made more for research and curiosity than to cause damages are now turning into sophisticated activities performed by individuals or criminal groups for profit or for political reasons. **The recent large scale attacks to countries like Estonia,[32] Lithuania[33] and Georgia[34] are the most widely covered examples of a general trend**.[35] The huge number of viruses, worms and other forms of "malware",[36] the expansion of botnets[37] and the continuous rise of spam confirm the severity of the problem: **ICT infrastructures are under constant attack** and, if Europe does not duly prepare itself, at all levels and by involving all stakeholders, the impacts from large scale attacks might be severe.

Compared to traditional security threat analysis, these types of threats have various features that make such attacks difficult to monitor, analyze, and counteract, such as the **difficulty in identifying attackers**, the **lack of boundaries**,[38] the **speed of technological development**,[39] the **low cost of tools to perpetrate attacks** and the emergence of automated methods for conducting them.[40]

In particular, the attacks that took place in **Estonia** exemplified how an attack on a CII can be launched from **any place** around the globe, by parties with **limited financial means** and **propagate** to a number of **essential/vital services**. Estonia, a highly connected nation, was the target of a two-week attack on various elements of its Internet infrastructure. As a result, the Parliament was forced to close down its e-mail system for 12 hours and the Estonian mass media stopped answering foreign calls. Due to extensive access attacks two major Estonian banks (Hansabank and SEB Eesti Unisbank) completely stopped their online business and blocked their contact with foreign countries for a long time. There have also been reports of attacks on the Estonian telephone system stating that at least one public telephone exchange was put out of service.

2.1.4. The fundamental problem and its underlying drivers

As CII are global, tightly interconnected and interdependent with other infrastructures, their security and resilience can not be ensured by **purely national and uncoordinated approaches**.

Moreover, the problems that this policy initiative aims to address are not limited to the European Union. As discussed above, threats and attacks to CIIs can take place from anywhere in the world.[41] It is therefore imperative to keep well in mind the global dimension of these issues, while at the same time remembering that immediate action is limited to the EU, as any form of international negotiation, agreement or consensus – which this policy initiative anyhow includes as a necessary, but prospective step – will both take a significant amount of time and will be

---

32 See footnote 31.

33 See Annex 18 A.

34 See Annex 18 B.

35 See *inter alia* Symantec, Internet Security Threat Report Volume XIII: April, 2008, available at http://www.symantec.com/business/theme.jsp?themeid=threatreport; Finjan, Web Security Survey Report – H1/08, available at http://www.finjan.com/content.aspx?id=827; Arbor Networks, Worldwide Infrastructure Security Report, 2008 (as well as Arbor Networks' Active Threat Level Analysis System at http://www.arbornetworks.com/en/atlas.html) – and, in general, the past editions of the report mentioned here, which give a good understanding of the general upward trends in disruptions and attacks to ICT systems and CII.

36 Malware is a commonly used abbreviation for for malicious software and "is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, whether it's a virus, spyware, et al" – see http://www.microsoft.com/technet/security/alerts/info/malware.mspx.

37 Botnets – which played a major role in the Estonian attack, as explained in Annex 16 – are made up of large numbers of computers that malicious hackers have brought under their control. While most owners are oblivious to the infection, the networks of tens of thousands of computers are used to launch spam e-mail campaigns, denial-of-service attacks or online fraud schemes. At the 2007 Davos World Economic Forum a senior Internet expert estimated that up to one quarter of all personal computers connected to the Internet may be used by cyber criminals in botnets, a level which would put the whole Internet at risk. The spread of botnets is likened to a pandemic, probably affecting 100-150 million of the 600 million computers connected at that time. See ENISA Position Paper No. 3 "Botnets – The Silent Threat", available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_botnets.pdf.

38 In the case of cyber attacks, the originator is often not located in the country of its target, and it might be difficult for law enforcement agencies in the target country to successfully intervene to block and/or prosecute the attackers.

39 In 1999, the Melissa virus took three days to spread across the Internet; in 2001, the Code Red worm took minutes. See Cukier, Schönberger, Branscomb, "Ensuring (and Insuring) Critical Information Infrastructure Protection", 2005.

40 Cavelty, 2007,"Critical information infrastructure: vulnerabilities, threats and responses".

41 The reports quoted in footnote 35 give a good overview of the extent of geographical scope of threats and attacks.

possible only if the European Union as a whole can show that is invested significant efforts into achieving what it might be requesting from other international partners.

Presently, **there are still notable discrepancies in the way in which Member States approach the problem of ensuring the security and resilience of CII, in the availability of operational tools to manage incidents, in the concrete functioning of the arrangements involving the private sector, and in the awareness of the broader Internet security and resilience problems**.

This is compounded by a general lack of incentives and sometimes of practical capacity for the private sector to invest in security at the level that governments would normally demand. In fact, **it is a common perception that market forces do not provide sufficient incentives to private operators for investing to protect CIIs at the level that governments would normally demand – a market failure**.[42]

The fundamental problem is that the low level of protection in some Member States has the potential to increase the vulnerability of others, and, in parallel, the lack of systematic cross-border co-operation substantially reduces the effectiveness of countermeasures.

In a networked world where systems continuously exchange information with one another or depend, at one level or another, on other systems, it is unavoidable that a higher level of vulnerability of one system might influence negatively other interconnected systems. This might be the case, for example, if a CII is taken control of by a malicious attacker, who then uses such infrastructure as a basis to launch attacks against other CII, located in different Member States, mirroring what is already happening today with the so-called botnets.[43]

A **number of underlying causes contribute to the general problem** outlined above:

- the **uneven approach among Member States to public policies related to the security and resilience of CII**
- the **difficult uptake of new, Europe-wide governance models**
- a **limited European early warning and incident response capability**
- a **low awareness on the risks for Internet security and resilience**

On top of this, there is a horizontal problem which interacts with the four phenomena above in a negative feedback-loop (i.e. the four issues above tend to exacerbate it and viceversa), i.e. the **lack of trustable data.**

All these problems have potentially far reaching consequences, affecting citizens, businesses and government entities across the Union, as the disruption of CII could ultimately entail loss of human lives, damages to property, and a collapse in public confidence and morale. It is therefore vital that proper measures to enhance the level of security and resilience of CIIs are taken, and that such measures are based on a proper risk assessment/management approach which is necessary to cope with problems/issues that are unknown or even unforeseen. To this end, it would also be important to examine the role of insurance mechanisms.

2.1.5. Uneven approach among Member States to public policies related to the security and resilience of CII

Member States' critical information infrastructures are currently subject to a number of different protective measures and obligations. However, the level of expertise and preparedness does not seem to be evenly distributed among Member States.

Consultations with Member States have shown significant differences regarding their national approaches to enhance the security and resilience of CII:

---

42 See J. J. Andersson and A. Malm, *Public-private Partnerships and the Challenge of Critical Infrastructure Protection*, in Isabelle Abele-Wigert and Myriam Dunn (eds.), *International CIIP Handbook 2006 vol.2*, Center for Security Studies, ETH, Zurich, 2007.

43 See footnote 37.

- the very understanding of what constitutes a CII differs across Member States;
- the **criteria and procedures for the identification of CII** vary from a top-down approach to a multi-stakeholder identification process, involving the private sector in risk assessment exercises;
- the institutional frameworks adopted at the national level differ;
- not all Member States have established **dedicated bodies**, dealing exclusively with CII issues, designed taking into account the national civil defence tradition, the amount of available resources, the historical experience, as well as the severity of the threat perceived by policy-makers;
- finally, while the **cross-border, pan-European** dimension of the security and resilience of CII is widely recognized in principle, not all Member States have developed a specific approach to identify and analyse the relevant domestic implications or have established a systematic dialogue with other Member States on this subject.

The existence of significant differences across Member States was also confirmed by a recent analysis, conducted by the **European Network and Information Security Agency** (ENISA)[44], on policies and regulations related to the resilience of public electronic communications networks.[45]

While it is clear that **each Member State has a domestic responsibility in addressing these challenges**, due consideration must be given to the fact that without a common understanding of the public policy implications, of the good practices in this field and of the 'lessons learnt' by others, **it is difficult to enhance across Europe the security and resilience of CII, which are intrinsically trans-national and, in some cases (such as the Internet) global**.

The differences existing among Member States can, therefore, constitute a major **obstacle to the implementation of appropriate EU-wide mechanisms to enhance the security and resilience of CII**, notwithstanding the fact that there are clear commonalities concerning the challenges and the issues faced by Member States, so that a more coordinated approach will benefit all.

In addition, the multiplication of requirements can imply a cost burden on private operators which have a presence across the EU or even globally. It might hinder the capability of EU businesses to provide an adequate and consistent level of protection of CII on a community-wide basis. This may in turn lead to even more fragmentation and lack of competitiveness of the European Union as a whole and affect the wealth creation capabilities of the European single market.

2.1.6. Difficult uptake of new European governance models

The concept of "governance" is interpreted in different ways, depending on the specific area in which it is used and on the particular actor putting it into practice.[46] In the context of this Impact Assessment**,** governance is understood as referring to **the set of practices and processes and various institutions and organisations, whether public or private, put in place in order to allocate resources related to the security and resilience of critical information infrastructures**.

Enhancing the security and the reliability of CII poses peculiar governance challenges, both nationally and at the EU level. This is particularly true given the privatisation of public utilities, which has substantially reduced government involvement in the direct management or control of

---

44 See http://enisa.europa.eu/, as well as section 3.3 of this report for a brief description of ENISA.

45 ENISA, Stock Taking of Member States' Policies and Regulations related to Resilience of public eCommunications Networks", September 2008, available at http://www.enisa.europa.eu/doc/pdf/resilience/stock_taking_final_report_2008.pdf. A thorough analysis of the findings of this report was conducted by ENISA, which delivered its final report in December 2008.

46 For example, the World Bank defines "governance" as "the traditions and institutions by which authority in a country is exercised for the common good. This includes (i) the process by which those in authority are selected, monitored and replaced, (ii) the capacity of the government to effectively manage its resources and implement sound policies, and (iii) the respect of citizens and the state for the institutions that govern economic and social interactions among them". Others refer to governance as the use of institutions and structure of authority to allocate resources and coordinate or control activity in society.

many CII. **Governments remain ultimately responsible for defining CII-related policies and for facilitating related information and communication processes,** but the involvement of the private sector is essential for **the concrete implementation of such policies**.

To address this governance problem **public-private partnerships (PPPs) have emerged as the reference governance model because they seem the most reasonable mechanism to manage the peculiar combination and intersection of governments' and private sector's role and responsibilities**.[47] However, PPPs are quite challenging to implement in practice, **as information exchange mechanisms between governments and the private sector basically become a trust issue**. Private companies will share their sensitive information, about critical assets and the problems they have faced, with other stakeholders (including governments) only if such information is treated confidentially and if they do not feel that what they say "will be used against them". Further key questions concern the **degree of institutionalisation of the process**, the **nature of information to be exchanged**, the **incentives to facilitate PPPs** and the fact that **CII can be owned or managed by foreign actors**.

However, although there is a general consensus that PPPs – which can range from extremely 'light' mechanisms, such as mere industry consultations on specific issues, to more formalized agreements[48] – can be a workable solution, **the European dimension of such an approach has not materialised so far**.

There is a disconnection between the need to address common European challenges in a coordinated fashion and the practical recognition that a proper dialogue between the public and the private sector is vital in order for public policy decisions to turn into operational reality on the ground.

2.1.7. Limited European early warning and incident response capability

The ARECI study highlighted several shortcomings in the European systems of early warning and incident handling. **Some Member States do not routinely receive network security incident reports**, although response and reporting is done informally among some operators. **In addition, some Member States have not established an authorised organisation as a focal point to receive and process such reports. This hinders early warning on incidents and problems related to the security and resilience of CII**.

Disaster recovery arrangements across national boundaries are limited and pre-arranged disaster recovery planning, exercises and assessments across national boundaries are hardly ever found. As a result, during disasters, **mutual aid is too often on an *ad hoc* basis**,[49] which in turn delays network and service recovery considerably.

From a technical perspective, **incident response concerning computer networks is managed primarily in Europe by dedicated facilities like Computer Emergency Response Teams** (CERTs).[50] CERTs are responsible for the understanding of vulnerabilities and threats, the monitoring, anticipation and response to possible critical events and the alert of relevant target groups.

CERTs are not homogeneous entities, since existing facilities display different characteristics regarding ownership, services provided, constituency served and technical capabilities.[51] **National CERTs**, for example, **represent the point of contact for a whole nation.** Sometimes

---

47 See, for example, Annex G to the OECD Seoul Declaration on the Future of the Internet Economy, where the establishment of "trusted public-private partnerships with a focus on risk" is explicitly recommended.

48 See Annex 9 for examples of PPPs in Member States.

49 As was the case, for example, of the Estonian attacks (See Annexes 7 and 16, as well as Gadi Evron, Battling Botnets and Online Mobs – Estonia's Defense Efforts during the Internet War, Georgetown Journal of International Affairs, Winter Spring 2008, available at http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf, and SEMA, Large scale Internet attacks – The Internet attacks on Estonia – Sweden's emergency preparedness for Internet attacks, 2008, available at http://www.krisberedskapsmyndigheten.se/upload/3040/Large%20scale%20Internet%20attacks_utb-ser_2008-2.pdf).).

50 Sometimes also referred to as Computer Security Incident Response Teams (CSIRTs).

51 ENISA, *CERT cooperation and its relevant facilitation by relevant stakeholders*, Deliverable WP2006/5.1 (CERT-D3). In particular, note that the term "governmental CERT" is used in this text as a synonym of "Governmental sector CERT/CSIRTs" in the taxonomy proposed by ENISA.

this task is fulfilled by **governmental CERTs**,[52] which serve all governmental agencies and organisations and possibly all public-sector bodies.

In terms of CERT cooperation platforms, the largest global CERT network is the *Forum of Incident Response and Security Teams* (FIRST), with about 200 members from around the world. In the EU, a cooperation platform between CERTs – the TF-CSIRT - was set up under the Trans European Research and Education Networking Association (TERENA).

However, co-operation and information sharing between **government-level entities** appears **under-developed**. The **most significant activity in the EU is represented by the European Governmental CERTs group (EGC[53])** which is, however, organized as an informal gathering. Moreover, **it was reported that there is still an evident gap in the degree of development of info-sharing and early warning co-operation mechanisms across sectors**.[54] Accordingly, this was identified as a priority area of intervention by, amongst others, the OECD.[55]

In short**, information sharing of security incidents between Member States is limited and largely informal, suffering from a lack of** well-established and trusted sharing and co-ordination mechanisms, due *inter alia* to potential legal issue in exchanging data on security incidents. These mechanisms **necessitate all National/Governmental CERTs to be well-functioning, i.e. have a common baseline in terms of capabilities**.

Besides information sharing on security incidents, **exercises and practical simulations are a key element in enhancing the security and resilience of CII**. **In the EU, cyber-security exercises are still in embryonic state**. Isolated instances exist only in some Member States which have also conducted trans-national exercises.

2.1.8. Low awareness about Internet security and resilience risks

Member States generally consider the Internet as a CII because the services and functions provided through the Internet are increasingly central to the economy and the society. **Its cross-border nature and the convergence of the different telecommunication and data networks are magnifying factors**. It has to be noted, however, that there is no consensus or agreement on what exactly the Internet **is** in this context. Some Member States only refer to the provision of services that run atop the Internet, while others include the underlying physical and logical infrastructure. **This divergence of views on the nature of the Internet and on the criticality of its different elements partly explains Member States' different (and sometimes conflicting) positions in international fora and their level of interest in the matter**. This, in turn, can hinder a proper prevention for, preparedness to and ability to recover from threats affecting the security and reliability of the Internet – all activities which, given the nature of the medium, have to be tackled keeping well into account the international dimension.

The Internet, thanks to its distributed, redundant design (originating in the '70s in order to resist nuclear strikes) has proven so far to be a **fairly robust and resilient infrastructure**.

However, it is fair to **question** its capability to continue withstanding the **rising number** of disruptions and cyber-attacks, especially considering its **phenomenal growth** across the globe, which, in turn, has produced a **growing complexity** of its physical and logical connections and the **emergence of new services and uses** that were not originally envisioned.

---

52 While in the early 90s academic CERTs were prevailing, and in the second half of 90s business and national CERTs were being developed, the establishment of governmental CERTs occurred mostly in the 2000s, with varying degrees in different Member States. Their diffusion can be associated with the progressive IT-enabling of public administration and scaling up of e-Government practices. At the same time, however, the establishment of Governmental CERTs indirectly reflects Member States' increasing awareness of the critical role played by CII for national security and socio-economic stability. For an overview on the situation of governmental CERTs in the European Union as of April 2008, cf. http://www.enisa.europa.eu/pages/CERT_map.html.

53 See http://www.egc-group.org/.

54 ENISA, *CERT cooperation and its relevant facilitation by relevant stakeholders*, Deliverable WP2006/5.1 (CERT-D3), pp. 46-49. These findings are then incorporated as a premise for the ENISA feasibility study on *European Information Sharing and Alert System*, p. 8.

55 OECD, *The Development of Policies for the Protection of Critical Information Infrastructures (CII). A comparative analysis in four OECD countries: Canada, Korea, the United Kingdom and the United States*, Working Party on Information Security and Privacy, 2007.

The connectivity infrastructures of the Internet and the services running on top of it can be subject to a variety of attacks. Of particular interest for activities aimed at enhancing the security and resilience of critical information infrastructures is the **extremely distributed** nature of the Internet, where end-nodes can be – willingly or unwillingly – be used as vectors of attacks, as is the case for **botnets**.

At the same time, this distributed nature is a reminder **that although a formalised and coordinated approach to incident response might be necessary in order to guarantee the proper response in case of widespread incidents, all options must be kept open when it comes to devising the specific forms of such coordination**. In some cases, as highlighted by the recent case of "route hijacking" in Pakistan,[56] the **distributed nature of control points typical of the Internet environment can help a faster recovery than would normally be the case when over-formalised procedures are put in place**. This calls for a **cautious**, **case-by-case analysis** of the proper public policies and operational procedures to be put in place to ensure the security and resilience of the Internet.

Instability or disruption of the Internet infrastructure can be also caused by natural events or physical disruption. This was the case of the **submarine cable cuts** that took place near Alexandria, Egypt, on 30 January 2008, in the Persian Gulf on 1 February 2008 and between Sicily and Tunisia on 19 December 2008. These disruptions, while not uncommon (only in 2007 there were fifty similar incidents in the Atlantic ocean[57]) significantly impacted the capability of Internet operators to communicate across different countries, including between the EU, Northern-western Africa and parts of the Middle East.[58]

As a matter of fact, Internet security and resilience has recently become a cause of increasing concern in some countries. **There are some voices stating that the Internet's present resilience might not be sufficient to face 'really extraordinary situations' causing an exponential increase of traffic on its infrastructure.** For example, a recent US Government Accountability Office report[59] states clearly that "it is possible that a complex attack or set of attacks could cause the Internet to fail." **Europe has become increasingly aware of the problem after the Estonian attack in 2007**,[60] which caused the temporary paralysis of Internet communication within the nation, demonstrating the vulnerability of Internet-based economic, social, financial and political infrastructures.

2.1.9. The lack of trustable data

It is extremely difficult to obtain reliable and trustable data related to security incidents, including on their actual occurrence, their impact (both in economic and social terms), the reactions that have been put in place by various actors, etc.

The underlying cause of this lack of data lies in the peculiar nature of the field: when it comes to security – including network and information security – **those who have the best access to relevant data on incidents**, actual losses incurred, investments, etc (e.g. network operators) **do not always have the proper incentives to disclose such data**. This might be due to concerns of business confidentiality, market confidence, political image and similar issues. Moreover and particularly in the context of policies aimed at enhancing the level of security and resilience of CII, **many relevant activities are performed by states for purposes of national security**. It is understandable that obtaining relevant data in these conditions is particularly difficult.

---

56 The incident took place because of the misconfiguration of an Internet "router", causing a large part of traffic to be diverted out of its intended destination (YouTube servers) towards an Internet Service Provider in Pakistan. See RIPE, *YouTube Hijacking: A RIPE NCC RIS case study*, 28 February 2008, available at http://www.ripe.net/news/study-youtube-hijacking.html.

57 See The Economist, *Of cables and conspiracies*, http://www.economist.com/world/international/displaystory.cfm?story_id=10653963.

58 According to RIPE, immediately following the cable cuts of January-February 2008, some networks became unreachable. Other sites were rerouted to circuits set up over other, lower bandwidth or longer distance cable systems. Both types of back-ups experienced increased latencies and congestion, significantly impacting end-users. For the full analysis by RIPE, see http://www.ripe.net/projects/reports/2008cable-cut/index.html. Analysis of the effects of the cable cuts of December 2008 is still ongoing (see http://www.telegeography.com/cu/article.php?article_id=26599&email=html).

59 *Internet Infrastructure: Department of Home Security Faces Challenges in Developing a Joint Public/Private Recovery Plan* (GA0-06-672 and GAO-06-1100T) June/September 2006.

60 See footnote 31.

This is a **known problem**, which was already highlighted by the Commission in COM(2006) 251 and in its related Impact Assessment.[61] In this Communication, the EC highlighted how "in order to successfully tackle the problems described above, all stakeholders need reliable data on information security incidents and trends. However, **reliable and comprehensive data on such incidents are difficult to obtain for many reasons, ranging from the rapidity with which security events can happen to the unwillingness of some organisations to disclose and publicise security breaches**. Nonetheless, one of the cornerstones in developing a culture of security is improving our knowledge of the problem".[62]

This is one of the reasons why the **Commission requested ENISA to perform a feasibility study of a "trusted partnership" with Member States and stakeholders to develop an appropriate data collection framework**, including the procedures and mechanisms to collect and analyse EU-wide data on security incidents and consumers confidence. The conclusions of the ENISA report[63] confirmed this point – to quote, "a wealth of data on information security incidents and consumer confidence already exists. **Often the question is where to find it and then how to obtain access to it. No-one wants to share information about embarrassing security incidents**. Moreover, those who invest in data collection initiatives want a return on their investment. **Collecting, aggregating and sharing data needs a sustainable business model**. The conclusion for decision-makers is that, if they want data about security incidents, they have to express this demand clearly – and they have to pay for it".

Moreover, as an **additional measure** to address the difficulty described here, the Commission plans to **launch in 2009 a study** entitled "development of a methodology and research of quantitative data on the economic impacts of the security and resilience of Critical communications and Information Infrastructures (CII)". The study will focus on **the analysis of the market forces and incentives for the stakeholders**, in particular the private sector, for investing in securing CIIs and on the **economics impact of disruptions**, aiming to gain a better insight into the direct and indirect economic impacts, on the society and economy at large, of disruptions of CII.

2.2. Who is affected, in what ways, and to what extent?

As discussed above, ICT infrastructures are increasingly becoming **pervasive** to the functioning of the entire economy and of society. **The problems examined in this Impact Assessment, therefore, potentially affect all European Union citizens, businesses and governments/public administrations**.

There are several different types of consequences for the various stakeholders that can be considered. These include:

2.2.1. Citizens

Individual users or consumers of ICT infrastructures expect a high level of infrastructure resilience and availability of all services without interruptions.

The costs of disruptions to individual consumers are difficult to measure, but they are likely significant. One example is the United States where consumers paid as much as USD 7.8 billion over two years to repair or replace information systems infected with viruses and spyware.[64]

Citizens would have to finance, through taxes, higher governmental expenses due to varying and uncoordinated protection and remediation measures, or would incur reduced levels of governmental services because resources are re-allocated to such measures without proper planning. It is also likely that any increased costs for businesses, such as implementation of incoherent security measures which differ from country to country, will be passed on to them through increased prices of access to ICT infrastructures.

---

61 SEC(2006) 656.

62 COM(2006) 251, p. 6.

63 Carsten Casper, *Examining the Feasibility of a Data Collection Framework*, ENISA/TD/ST/08/0001, November 2007.

64 See the September 2006 issue of "Consumer Reports" http://www.post-gazette.com/pg/06225/712889-96.stm.

Moreover, having in mind the high and growing penetration of e-government services, as well as the widespread usage of ICTs as a support to 'standard' administration and governmental functions, the impact on citizens of a large scale incident might be quite high.

Last, not least, it should be kept in mind that more and more personal data of citizens are communicated and transmitted via CII. Inadequate security measures could lead to loss of sensitive personal information and pose the risk of identity theft or other fraud. In October 2007, a major loss of citizens data occurred in the UK as two computer discs with 25 million child benefit records, complete with sensitive personal information, were lost from Her Majesty's Revenue and Customs department.[65] **Enhancing the security and resilience of such infrastructures is, therefore, absolutely vital for the protection of citizens' personal data and the proper enforcement of the right to privacy**.

2.2.2. Businesses

In case a CII is disrupted, business activities relying on the access, timely delivery and or integrity of information – which includes both new ICT-intensive and "bricks and mortars" businesses – might suffer immediate financial losses and a longer term opportunity cost related to the loss of consumer trust and confidence.

The costs associated with infrastructure disruptions can be seen as direct and indirect costs. **Direct costs** can include the loss of value in assets that are destroyed, stolen, compromised, or otherwise degraded; the expenses incurred in restoring the system to its original state (i.e. extra spending on labour and materials); the costs resulting from business interruption (i.e. lost revenue and loss of productivity during the disruption); lost sales (both short-term, limited to the attack period, or long-term, as a result of customers switching permanently to competing firms), etc. [66]

Disruptions may have also **indirect costs**, which may continue to accrue after the immediate damage is repaired, such as loss of reputation, or damage to a firm's brand. A March 2000 survey by Gallup suggests that consumer confidence in online shopping was hurt by attacks on prominent sites: a third of online consumers overall said they might be less likely to make a purchase via the World Wide Web in light of the attacks that had blocked access to such Web sites as Yahoo and Amazon.[67] Customers may defect to competitors, financial markets may raise the firm's cost of capital, insurance costs may rise, and lawsuits may be filed.

Investigations into the impact of cyber-attacks on stock prices show that identified target firms suffer losses of 1%-5% in the days after an attack.[68] For the average New York Stock Exchange corporation, price drops of these magnitudes translate into shareholder losses of between $50 million and $200 million.

Moreover, for businesses it is important to have a level-playing field on which to compete. Therefore, it is less likely that they would invest in sufficient security if their competitors are not subject to the same costs and obligations as this would put them at competitive disadvantage.

2.2.3. Governments and public administration

Governments and public administrations are responsible for a country's overall security, public safety, the effective functioning of the economy, and the continuity of government services. More and more, governments and public administrations rely on information infrastructures for their operations and a disruption of such infrastructures might therefore negatively impact their capability to provide these services. This would have an effect both on governments/public administrations themselves and on public confidence.

---

65 http://www.timesonline.co.uk/tol/news/uk/crime/article4211711.ece.

66 In the US, for example, the Business Roundtable estimated that for the companies it surveyed (with an average of 62,500 employees) a one-month Internet disruption would result in an estimated $27.9 million of lost productivity. In addition, an average Business Roundtable company with annual revenues of $31 billion and deriving 10% of its revenues from Internet transactions would suffer from lost sales for one month of around $63.7 million (see Business Roundtable, "Internet Business Dependence Report", 2007). A survey for UK shows that the average total cost of a UK company's worst incident in 2007, was in the range of £8,000 to £17,000. For large businesses, the average cost was between £65,000 and £130,000, whereas for very large respondents it averaged roughly £1 million, with business disruption being the largest component (see BERR, Information Security Breaches Survey 2008, conducted by PricewaterhouseCoopers).

67 KPMG International, "E-commerce and cyber crime: New Strategies for Managing the Risks of Exploitation".

68 Information based on the working document "The Economic Impact of Cyber-Attacks" (see annex 19).

Moreover, notwithstanding the increasing usages of e-Government services it should not be forgotten that even for those public services which are not directly available to the public via ICTs, the latter are an essential element of the "back office". The disruption of such infrastructures would create major problems for the normal operations of public administration and governmental services.

These potential impacts must be analysed in the context of recent findings: the latest Symantec security reports highlight that **an increasing number of attacks were targeting governments**, accounting for 60% of all the attacks worldwide during the second half of 2007. During the previous half-year, this type of attacks accounted for the 12% of the total.[69] The high number of attacks targeting governments is further confirmed by the US Department of Defence.[70]

2.3. How would the problem evolve, all things being equal?

Without horizontal actions at EU level, Member States would continue acting individually or in the frame of bilateral or regional agreements. Member States recognise the relevance of ICTs, its importance for society and the strategic value of enhancing the security and resilience of CII. On the other hand, some Member States might face difficulties in defining the critical issues that need immediate actions, especially when there is a need to prioritise them according to available resources.

Consequently and notwithstanding the existing initiatives at EU level (see section 3.3 below) there would be a strong risk linked to the evolution of different national approaches which might turn out to be incompatible. At national level, Member States would continue to address these issues at their own pace. As a result, businesses would refrain from investing in security issues, as the existence of a multitude of standards and obligations would decrease their competitiveness. Due to the cross-border characteristic of the problem, the differences in protection measures among the Member States would mean that vulnerability levels would remain quite high or possibly rise, despite increased individual efforts.

In addition to being diverse and uncoordinated, existing measures at national level are sometimes insufficient. While most Member States have established National/Governmental CERTs, their expertise and operational capability differ, and there is no efficient cooperation among them. The persisting lack of cooperation at EU level would leave Member States in a situation where they have to address alone problems of cross-border nature.

Currently, at EU level, there are a number of initiatives with relevance to critical infrastructures which complement the initiative on CIIP and vice versa, but at the same time have different objectives and timeline. The Directive on European Programme for Critical Infrastructure Protection (EPCIP)[71] addresses the identification and designation of European Critical infrastructures. The CIIP initiative is the ICT sector-specific approach with a focus on security and protection. Another initiative in this area is the Critical Infrastructure Warning Information Network (CIWIN). It represents a tool for rapid alert that enables participating Member States and the Commission to post alerts on immediate risks and threats to critical infrastructure, whereas the CIIP initiative aims at engaging all relevant stakeholders in cooperation with a much broader scope. Thus, if no additional action is undertaken at EU level with relevance to critical information infrastructures, i.e. an information and alert sharing system envisaged under the proposed CIIP initiative, no existing tool would to engage operationally public and private sector stakeholders in handling attacks/disruptions and targets, in particular, citizens and SMEs.

On the international level, there are no adequate mechanisms which address the objectives of the initiative. The events in Estonia, Lithuania and Georgia proved that trans-national cooperation was needed to resolve the problems. Due to the lack of established mechanisms, however,

---

69 No comparable figures are available for the previous years, so that it is impossible to conclude whether this exponential increasing in attacks against Governments represents a consolidated trend or an anomalous peak.

70 "*Last year, the Department of Defence suffered an estimated 80,000 network attacks. On government networks alone, a new software vulnerability is exploited every 82 minutes. Meanwhile, attacks on US federal agencies' computer systems are increasing at alarming rates. Furthermore, Government utilities are being hit by an estimated 500 to 1000 attacks from hackers and malicious code every year.*" Cyber security: missions, opportunities, initiatives and risks. Announcement of a conference to be held in Washington, D.C. - June 9-10, 2008 - http://www.ttcus.com/view-about.cfm?id=66.

71 2008/114/EC

cooperation would continue to be on an ad hoc basis which does not seem to be the most efficient way when time is a critical factor.

2.4. Does the EU have the right to act and is EU added-value evident?

2.4.1. Right to act

The EC Treaty identifies in its **Article 2** a number of objectives, whose attainment could be facilitated by enhancing the security and resilience of CII in Europe, i.e. to promote (a) a harmonious, balanced and sustainable development of economic activities, (b) a high degree of competitiveness, (c) a high level of protection and improvement of the quality of the environment, (d) the raising of the standard of living and quality of life and (e) solidarity among Member States.

Moreover**,** enhancing the security and resilience of ICT infrastructures to achieve a high and effective level of network and information security within the Community is an important element contributing to the smooth functioning of the internal market.

Therefore, **in accordance with the European Court of Justice jurisprudence,**[72] **Article 95 of the EC Treaty** is to be considered as the appropriate legal base for the adoption of (binding) measures to achieve a high and effective level of security and resilience within the Community.

In addition, national security concerns play an important role in defining network and information regulations and obligations relevant to security and resilience of ICT infrastructures. This leads to a multitude of different national regulations that hinder the capability of EU businesses to economically provide an adequate and consistent level of security and resilience of ICT infrastructures. This may in turn lead to fragmentation and thus affect the competitiveness of the European Union as a whole and the wealth creation capabilities of the European single market.

Besides having its immediate legal basis on article 2 and on article 95 of the EC Treaty, this policy initiative gives additional substance to a number of ongoing initiatives at the EU level. These are discussed in more detail in Section 3.3 below.

2.4.2. Subsidiarity principle

The differences in the state of awareness and the level of preparedness across Member States are particularly problematic for the ICT sector: in a world where bytes and bits travel often at the speed of light from one point to another, **a lack of security in one node can become a major problem for another node**. **If a Member State is not duly prepared to cope with cyber-attacks to its infrastructure, it could easily become a basis and a vector of attack to the infrastructures of another country**. Botnets are a clear example of this problem. **The security of a complex, interconnected system is only as high as the "weakest link of the chain"**. It is therefore in the interest of all Member States and of the Union as a whole to make sure that all "links" are at the same – high – level of network and information security and preparedness.

At the same time, **no Member State is an island**. The global nature of the Internet, which is the most evident example of an interconnected CII, requires a holistic and global approach to network and information security. **At EU level it is possible and necessary to have a direct impact; international cooperation will build on effective action at this level**.

Because of the high interconnectedness between CII and societal systems, which rely upon CII, it is unfeasible, ineffective and counterproductive, and would run against the basic principles underlying the European Union, for each Member State to only guard its own backyard. **A failure in one Member State will unavoidably produce effects in another. This is why it is necessary for all the Member States to coordinate their efforts in one direction and to try and achieve a satisfactory level of preparedness with a similar timescale**.

[72] See Case C-217/04, United Kingdom v Parliament and Council where the European Court of Justice upheld the decision to base the creation of the European Network and Information Security Agency on Article 95 TEC. This judgment confirms that the EC Treaty confers on the Community discretion on the range of measures to be adopted with regard to the attainment of the internal market.

The Community (and international) dimension of the problem implies that when investigating the weaknesses and vulnerabilities and identifying gaps in protective measures, **an integrated EU-wide approach to the enhancement of the security and the resilience of CII would usefully complement and add value to the national programmes for critical infrastructure protection already in place in the Member States as well as bilateral and multilateral cooperation schemes between Member States**. Many of the challenges and the issues faced by Member States are similar and thus a common approach would benefit all.

For the reasons stated above, the proposed policy action fully respects the principle of subsidiarity, in its dual dimension of respect for the added-value test (it would be difficult for any Member State to achieve the objective by itself) and of the boundary test (European action will be limited to what Member States cannot achieve satisfactorily by themselves, providing a framework for coordination and, where appropriate, complementing their activities).

2.4.3. Respect for fundamental rights

This initiative will contribute to the protection and the promotion of a number of fundamental rights, as recognised *inter alia* by the Charter of Fundamental Rights of the European Union, including the right to the **protection of personal data and privacy** (thanks to the enhanced level of security of infrastructures which are more and more used to store and process such data).

3. OBJECTIVES

3.1. What are the general policy objectives?

The **general objective** of this policy initiative is **to enhance the level of awareness and preparedness across the EU and to ensure security and resilience of CII as the frontline of defence**.

3.2. What are the more specific/operational objectives?

In order to achieve the general objective of the proposed policy, it is essential that relevant public and private stakeholders be engaged in ensuring that **adequate and consistent levels of preventive, detection, emergency and recovery measures are put in operation** to achieve an adequate level of **security and resilience of CII** and guarantee the **continuity of services**.

More specifically, on the basis of the analysis carried out, the general objective can be achieved through the attainment of **four specific objectives**, namely:

1. **Bridging gaps in national policies for the security and resilience of CII;**
2. **Enhancing European governance for the security and resilience of CII;**
3. **Strengthening Europe's operational incident response capability;**
4. **Enhancing Internet security and resilience.**

In particular, the **achievement of specific objective #1** will develop **awareness and a common understanding of the security and resilience challenges for CII; stimulate the adoption of shared policy objectives and priorities; reinforce cooperation between member States and integrate national policies in a more European and global dimension**. Achieving Specific Objective #1, which focuses on national approaches, will create the necessary basis to foster a European approach to the enhancement of the security and resilience of CII, which would complement and bring European value added to national policies and programmes

Building on top of national approaches, **specific objective #2** addresses the need to provide a **European-wide governance framework**, which is currently missing, to properly involve the private sector across Europe in the definition of **strategic public policy** objectives as well as **operational/tactical priorities and measures**. Such framework would take the form of a **Public-Private Partnership**.

At the same time, a higher level of preparedness must necessarily be based on a **strong European operational incident response capability**, which is the main aim of **specific objective #3**. Such capability would build upon, first of all, the existence of **well functioning National/Governmental CERTs in all Member States**. This will be a precondition for National/Governmental CERTs to act as national **catalysers of stakeholder interests and capabilities for public policy activities**, including those related to establishing national information and alert sharing systems to reach out to citizens and SMEs, and to engage in **effective cross-border cooperation and information exchange**, possibly leveraging existing organisations such as the European Governmental CERTs Group. The development of **national contingency plans** and the performance of **regular national and pan-European exercises** would be a necessary ingredient for the achievement of a good European operational incident response capability. In addition, regular exercising would strengthen the level of preparedness as it would put the focus on flexible strategies and processes rather than on ready-made solutions, which is important when dealing with the unpredictability of potential crises. In this respect, it would also help develop a proper risk assessment/management culture, which is necessary to cope with future threats and unforeseen problems.

Last, not least, the **specificities of the Internet**, i.e. the fact that it is an **intrinsically global** and **highly distributed**, with "control centres" not necessarily following national boundaries, calls for a specific, targeted approach in order to ensure its security and resilience, which is critical for Europe at large – this is the goal of **specific objective #4**. Two converging measures are necessary. Firstly, **to achieve a common understanding** across the EU on what are the

European priorities – both in terms of public policy and of operational deployment – to ensure the security and resilience of the Internet; secondly, **to engage the global community** in agreeing on a **set of principles** for Internet security and resilience, building upon strategic cooperation with third countries such as the USA, Japan and Canada and making sure that **European values** are preserved and promoted throughout the process.

The **operational objectives** that are needed to achieve each **strategic objective** are discussed in more detail below.

3.2.1. Specific Objective #1: bridging gaps in national policies for the security and resilience of CII

In order to achieve **specific objective #1**, the following **operational objectives** would have to be achieved:

Operational objective	Description
1.1: Enhancing the cooperation on policy areas that constitute the common ground of national approaches to the security and resilience of CII	The lack of common definitions and policy standards prevents Member States from **cooperating effectively** amongst each other and, at a later stage, to **pool their capabilities and resources** at the European level. Identifying the commonalities amongst Member States' policies would help each single Member States to build upon good practices and 'lessons learned'.
1.2: Information sharing and exchange of good policy practices	Once the commonalities amongst Member States are identified, it is necessary to enhance the efficiency and effectiveness of information sharing and the exchange of good policy practices. At this stage, the exchange would take place exclusively among Member States, to help foster a coherent framework of public policy approaches to the issues under consideration.

3.2.2. Specific Objective #2: Enhancing European governance for the security and resilience of CII

In order to achieve **specific objective #2**, the following **operational objectives** would have to be achieved:

Operational objective	Description
2.1: Knowledge sharing to deepen the understanding and mastering of challenges for the security and resilience of CII.	The **private sector** owns and manages the vast majority of communication networks and information infrastructures as a result of the privatisation of public utilities. At the same time **governments remain ultimately responsible** for defining and leading public policies for the security and resilience of CII. It is in this context that a number of Member States have already established national PPPs.[73] However, the global nature of the issues at stake calls for a **strong and trusted PPP at the European level**.
2.2: Identification and dissemination of good baseline practices	Identifying and disseminating the good baseline practices to be followed, in terms of industrial deployment, to ensure the security and resilience of CII is instrumental in enhancing the governance of the security and resilience. Policy makers should be able to receive reliable, precise and aggregate information on current security incidents or threats so that they can assess the policy risk posed by a certain situation and make informed choices accordingly. In addition, private stakeholders who are able to assess the risks for their business do not necessarily have sufficient information to assess the risk for the society as a whole. Private stakeholders therefore need to receive information and guidance from public bodies.

3.2.3. Specific Objective #3: Strengthening Europe's operational incident response capability

In order to achieve **specific objective #3**, the following **operational objectives** would have to be achieved:

[73] See Annex 9 for some examples of Public-Private Partnerships in Member States.

Operational objective	Description
3.1: The identification and agreement on a minimum level of capabilities and services for well-functioning National/Governmental CERTs and the establishment of well-functioning National/Governmental CERTs	While most Member States have already put in place National/Governmental CERTs or are in the process of doing so (an activity which should be encouraged by all means possible) it is vital that all such CERTs share a common baseline of capabilities and services, to be identified and agreed upon by Member States. Without such a common baseline, it would be extremely difficult – if not impossible – for National/Governmental CERTs to act coherently at the European level, share information and replicable good practices and, in general, provide the level of European response capability which is needed in order to face threats to CII in a coordinated manner, rather than in 'ad hoc' fashions. In addition, well-functioning National/Governmental CERTs would constitute the building blocks for national Information Security and Alert Systems (ISAS) to reach out citizens and SMEs. However, in order to benefit all EU citizens such national ISAS should be stimulated to share information and pool together expertises.[74]
3.2: Development of Operational Contingency Plans and Performance of Exercises	A protective program initiative specifically applicable to incident response functions should be developed and include the plans, programs, and mechanisms for identifying and refining requirements and developing reconstitution capabilities. **The concrete functioning of these plans should be tested in exercises involving both private and public actors** to ensure their maximum effectiveness in case of need, a better definition of situational roles in a real crisis and a proper understanding of risk assessment/management approaches necessary to cope with future threats and unforeseen problems.
3.3: Reinforcement of operational co-operation and dialogue between National/Governmental CERTs	Once a common baseline of capabilities for National/Governmental CERTs is agreed upon and achieved in all Member States, reinforcing CERTs cooperation across Europe is vital in order to ensure a coordinated response capability.[75]
3.4: Clarification of legal obstacles to the exchange of information on incidents and providing collaborative platforms for ensuring the confidentiality of information	Information related to security threats and incidents can often be of a sensitive nature, whether for commercial or national security purposes. This highlights the need to support the establishment of collaborative trusted platforms that may guide and clarify the cross-border sharing and exchange activities of National/Governmental CERTs.

.

74 It is in response to this need that the Commission announced in the Communication COM(2006) 251 the intention to ask the European Network and Information Security Agency (ENISA – described in sec. 3.3) to investigate the feasibility of a multilingual European Information Sharing and Alert Systems (EISAS) that would build on existing national systems and be of benefit for the EU citizens. The EISAS final report highlights both the benefit of fostering the dialogue among national information sharing systems as well as the need to take a step-wise approach to realise such a system (see http://www.enisa.europa.eu/doc/pdf/studies/EISAS_finalreport.pdf). To this end, earlier this year the European Commission launched a call for proposals for a prototype of a European multilingual information-sharing and alert system under the EPCIP financing scheme.

75 See *inter alia* ENISA, CERT cooperation and its further facilitation by relevant stakeholders, 2006.

3.2.4. Specific Objective #4: Enhancing Internet security and resilience

In order to achieve **specific objective #4**, the following **operational objectives** would have to be achieved:

Operational objective	Description
4.1: Defining EU priorities for Internet long term security and resilience	These would encompass the critical components affecting widely the functionality of the Internet as well as the overall architecture, the governance and international arrangements for remedial, mutual assistance and recovery. While policy makers should not be involved in the details of the operations to enhance the robustness of the Internet and response to incidents, they should ensure that all the conditions are in place for ensuring the long term stability and resilience of the Internet and define what the priorities are.[76] The output of this exercise could take different forms.
4.2: Launching a European-led international initiative with aim to create a set of principles for Internet security and resilience	Given the intrinsically global nature of vulnerabilities and threats, it is necessary to achieve a multi-stakeholder consensus at the EU level on governance issues related to Internet resilience and security with reference to international fora. Indeed, any measure with a local or even regional dimension would have very limited effect whenever the traffic could be routed through a country not covered by such a regulation. Respondents to the public consultation on an EU Strategy for International Co-operation on ICT highlighted that enhanced cooperation with third countries (especially with the US authorities) is absolutely necessary. The majority of Internet users and the most prominent sources of malware reside outside the EU. Enhanced EU-US cooperation on Network and Information Security was pointed out as a strategic mean to show the way and entice others to follow. This initiative would complement and liaison with the relevant fora where similar discussions are already taking place, such as the OECD, the ITU, the Security and Stability Advisory Committee of ICANN, etc. Although the precise form that could be taken by this initiative depend on the particular type of international engagement chosen – ranging from non-binding declarations to fully binding treaties – the key element that must me achieved is an international consensus on the key issues, challenges and actions needed to enhance the resilience and security of the Internet as the most apparent example of a global CII.

.

3.3. Consistency of the objectives with other EU policies

The events in Estonia,[77] Lithuania[78] and Georgia,[79] as well as the growing trend of threats, incidents and cyber-attacks that took place during the past years highlight the need for a strong and coordinated EU action. They also reinforce the necessity to take a more **holistic approach to enhancing the security and resilience of CII as an important safeguard to provide the first and most critical line of defence** against cyber attacks and disruptions.

The **enhancement of the security and resilience of ICT infrastructures is an important element** of the Commission policy on network and information security that was renewed with Communication COM(2006) 251 on a strategy for a Secure Information Society, whose main elements were endorsed by the Council in its Resolution of 22.3.2007.[80] This Communication

76 The availability and reliability of Domain Name System (DNS) services, the security of traffic exchange between operators (including BGP security), the need to measure and monitor network traffic, the security implications of the deployment of IPv6 and its coexistence with IPv4, the disclosure processes of Internet vulnerabilities and the need for enhanced coordination during Internet attacks are some examples of critical topics which were highlighted in the consultation process, and which should be addressed in the general process of definition of common EU priorities in this area.

77 See Annex 16.

78 See Annex 18 A.

79 See Annex 18 B.

80 Resolution 2007/C 68/01 of 22.3.2007, OJ C068 24.3.2007: *The Council welcomes the intention of the Commission to encourage the Member States to examine, via a multi-stakeholder dialogue, the economic, business and societal drivers with the aim of developing an ICT sector-specific policy to enhance the security and resilience of network and information systems, as a potential contribution to the planned European Programme on Critical Infrastructure Protection.*

defines also actions to strengthen the role, on more **tactical** and **operational** levels, of ENISA in support to the strategy.

ENISA was established in 2004 to ensure high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, private and public sector organisations of the EU, thus contributing to the smooth functioning of the internal market.[81] Since 2008, at the request of the Commission and some Member States, security and resilience of electronic communication networks has become a priority theme of the work programme of the Agency.

On the regulatory side, the Commission proposal to reform the Regulatory Framework for e**lectronic communications** networks and services[82] contain new provisions on security and integrity. **Of particular relevance is the proposal for Art. 13a and 13b of the Framework Directive, which includes provisions to strengthen operators' obligations** to ensure that appropriate security and integrity measures are taken to meet identified risks and to guarantee the continuity of supply of services. In addition, Art 13a includes provisions on mandatory breach notification. This regulatory approach is conducive, from a market legislation perspective, to the general objective of planned policy on security and resilience of CII. The Community legislature is currently discussing the Commission's proposal; both the European Parliament and the Council have been showing large support to the provisions included in Article 13a and 13b.[83]

Moreover, the goals pursued by the proposed initiative are fully **coherent** and, in fact, **conducive** to the general debate that is taking place on the **future of Network and Information Security**. This debate followed Commissioner Reding's calls on the European Parliament and the Council "to open, early in 2009, an intense debate on Europe's approach to network security and on how to deal with cyber-attacks", and the requests made both by the Parliament and by the Council for "a debate on the goals of a possible modernised network and information policy, and on the most adequate means to achieve them". In support to this debate, on 7 November 2008 the Commission has launched a public consultation that will run until 9 January 2009.[84]Although this consultation is not formally linked to the policy initiative being proposed here, there is a clear synergy between the two that would be leveraged upon.

The objectives of the proposed initiative are also fully consistent with, and provide a useful basis of information for, the **European Programme for Critical Infrastructure Protection** (EPCIP) framework, as explained in section 2.3 above.[85]

They are also complementary to existing **third pillar** initiatives – e.g. fight against cyber-crime – as envisaged *inter alia* by the Council Framework Decision on Attacks Against Information Systems that was adopted in 2005 (2005/222/JHA) with the aim to strengthen criminal judicial cooperation on attacks against information systems by developing effective tools and procedures. **As the proposed initiative focuses on prevention, preparedness and awareness from the perspective of enhancing the intrinsic security and resilience of CIIs, it does not conflict or duplicate the efforts under the third pillar, i.e. from the perspective of police and judicial cooperation** addressing measures to prevent, fight and prosecute criminal and terrorist activities targeting CIIs**.**

Last, not least, this initiative is synergetic with current and prospective **EU research initiatives** in the field of network and information security, as well as with **international initiatives** in this area.

From a **research perspective**, in September 2007 the **European Security Research and Innovation Forum** (ESRIF) was established. It will draw, possibly by the end of 2009,[86] a Joint

81 European Network and Information Security Agency - Regulation (EC) N 460/2004 of the European Parliament and of the Council of 10 March 2004.

82 COM(2007)697, COM(2007)698, COM(2007) 699.

83 European Parliament Legislative Resolution (P6_TA-PROV(2008) 0449) of 24.09.08 and the Report of the Working Party on Telecommunication and Information Society of the Council of the European union no. 15072/08 of 6 November 2008.

84 See http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464.

85 COM(2005)576 final of 17.11.2005.

86 See http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/346&format=HTML&aged=0&language=EN&guiLanguage=en.

Security Research Agenda containing *inter alia* recommendations to public authorities. **The public-private partnership proposed in specific objective #2 could clearly benefit from the work of ESRIF and would also provide valuable input to it**. Moreover, under the **ICT Theme of the 7th Framework Programme for Research and Development** the Commission is funding110 M€ over 2007-2008 for research in the area of Secure and trustworthy network and service infrastructures, with a focus on protecting the Internet and other ICT networks against emerging threats and vulnerabilities, addressing the assessment and management of security levels of networks, content and services, early detection, monitoring and countering of attacks and intrusions, and novel threat prevention mechanisms.[87] **The specific objectives #2 and #4 of this initiative would clearly benefit from the insights provided by these research activities**.

Regarding the **international dimension**, recognised principles like the G8 principles on CIIP[88], the UN General Assembly Resolution 58/199 'Creation of a global culture of cybersecurity and the protection of critical information infrastructures'[89] and the recent OECD Recommendation on the Protection of Critical Information Infrastructures[90] will be duly taken into account.

Moreover, the proposed policy initiative takes into account and does not duplicate the work conducted by **NATO** in the context of cyber-security – specifically the common policy on cyber defence and the activities of the Cyber Defence Management Authority (CDMA), announced by NATO on April 2008, as well as the outputs of the NATO Cooperative Cyber Defence Centre of Excellence[91] (CCD-COE), established in March 2008. **It is important to highlight the different nature of the NATO initiatives (with their main focus on military defence) *vis-à-vis* this proposal, which aims at structured coordination and cooperation of civilian (public and private) resources and capability in and across Member States.**

87 See Annex 6 for a more thorough description of the main EU research activities in this area.

88 See http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf.

89 See http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

90 See http://www.oecd.org/dataoecd/1/28/40821729.pdf, Annex G.

91 See http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD.

4. POLICY OPTIONS

The possible policy options that are examined in this Impact Assessment are:

1. **Business as usual**
2. **The implementation of measures within a non-binding framework**
3. **The establishment of a binding framework**

4.1. Option 1: business as usual

Under this policy option no further action would be undertaken at the European level, apart from those already running or envisaged (see section 3.3).

Member States would be left to address the problems examined here independently. As a result of the current and foreseeable trends, only very limited progress is likely to occur, leading possibly to more uncoordinated policy developments, limited cooperation between National/Governmental CERTs, a slow up-take of contingency planning and cyber-security exercises and the consolidation of national approaches to partnership and governance (mostly through "learning by doing").

4.2. Option 2: the implementation of measures within a non-binding framework

Under this policy option a non-binding framework would be proposed.
The non-binding framework would focus on providing the platforms and instruments to allow all stakeholders to coordinate their activities. Also, proper awareness raising activities would be put in place in order to raise the level of attention and sensitivity to the European dimension of the issues under discussion.

The framework would take the form of a Communication, which would be accompanied by an Action Plan, to engage Members States, the private sector and civil society in the actions needed to attain the overall objective of ensuring resilience of EU communication networks and information infrastructures. The Communication could be endorsed by the Council of the EU via a resolution or a recommendation. In addition, the European Parliament may also decide to contribute to the discussion.

The actions that would be put in place under policy option 2 are the following:

Operational objective 1.1 Enhancing the cooperation on policy areas that constitute the common ground of national approaches to security and resilience of CII	**Action 1.1.1** The Commission would work with Member States in identifying transferable examples of public policy practices and commonalities. Such activity would benefit from stock-taking and analysis of existing commonalities, building upon existing studies and analysis.
Operational objective 1.2 Information sharing and exchange of good policy practices	**Action 1.2.1** The Commission would establish a European Forum for Member States to share information and good policy practice on security and resilience for CII. The activity would benefit from the result of the work and operational activities conducted by other organisations (e.g. ENISA).
Operational objective 2.1 Knowledge sharing to deepen the understanding and mastering of challenges for the security and resilience of CII	**Action 2.1.1** The Commission would establish a European Public-Private Partnership, to support cooperation and information sharing on European and global challenges for the security and resilience of CII. The primary focus would be on the European dimension of the challenges for security resilience of CII, both from a strategic (e.g. good practices for public policy) and tactical/operational (e.g. industrial deployment) perspective. The specific form of this PPP should be decided together with all the involved stakeholders, but it should nonetheless be firmly based on four key principles: • **Complementarity**: the European PPP should build upon and complement both existing national initiatives as well as the work conducted by the European Network and Information Security Agency (ENISA). It should fully respect national responsibility, without duplicating efforts or putting unnecessarily burden or responsibility to participating parties.

	• **Trust**: It should provide the structure, processes and environment for "trusted collaboration", including the protection of information from disclosure. • **Value**: It should set emphasis on bi-directional exchanges between the public and private participants and provide value for both governments and industry. Industry and government requirements, priorities and objectives should be aligned. • **Not only competition**: Security and resilience of CIIs should not be a matter left exclusively to private competition, Topics to be discussed in the context of such partnership may include: • processes for vulnerability disclosure • practices for threat identification • methodologies for risk assessment • common terminology and procedures for the collection and dissemination of information on economic impacts of security incidents • workable frameworks and practices to support the exchange of sensitive information.
	Action 2.1.2 The Commission would analyse the methodological and legal challenges related to the collection and dissemination of information on the economic impacts of security incidents. To this end, a study on the economic implications of the security and resilience of CII should be launched in 2009, under the eCommunications budget line. The results of these activities would feed into the work of the European partnership planned in Action 2.1.1.
Operational objective 2.2 Identification and dissemination of good baseline practices	**Action 2.2.1** The Commission, using the European partnership planned in Action 2.1.1, would support the identification and dissemination of baseline requirements for security and resilience, good policy practices and measures related *inter alia* to industrial deployment and to the collection, aggregation and dissemination (among all stakeholders) of information on vulnerabilities and threats.
	Action 2.2.2 In the context of FP7 or other programmes, the Commission would launch, where appropriate, calls for research projects aimed at identifying prospective challenges (and possible solutions) to enhance the security and resilience of CII.
Operational objective 3.1 Identification and agreement on a minimum level of capabilities and services for well-functioning National/Governmental CERTs and the Establishment of well-functioning National/Governmental CERTs	**Action 3.1.1** The Commission would work with Member States on defining the appropriate baseline of capabilities, services and operational functions for National/Governmental CERTs. The definition and a wide adoption of such a baseline would reinforce the national response capability and ensure that national capabilities could cooperate at the European and international levels.
	Action 3.1.2 The Commission would encourage and support (*inter alia* by promoting good practices and guidelines) Member States to establish well-functioning National/Governmental CERTs with the aim to integrate their function/operation more in a public policy dimension. In addition to their operational function, National/Governmental CERTs could play the role of catalysers of stakeholder interests and capabilities for public policy activities, including those related to establishing national information and alert sharing systems to reach out to citizens and SMEs, which constitute the national building blocks for EISAS.[92] The activity would benefit from the work conducted by ENISA in the context of its CERT-related activities.
Operational objective 3.2 Development of Operational Contingency Plans and Performance of Exercises	**Action 3.2.1** The Commission would stimulate and support Member States in developing national operational contingency plans for CII. To this end, the Commission would organise meetings / conferences to exchange experience, lessons learnt and 'good practices'. The establishment of national contingency plans would be instrumental for stronger cooperation and coordination towards European-wide operational contingency plan. This activity would also be supported via the forum planned in Action 1.2.1, where common strategic objectives could be discussed. ENISA could be asked to support these exchanges by providing its expertise on the operational dimension of this challenge.
	Action 3.2.2 The Commission would facilitate the Member States to design and perform pan-European exercises to test contingency plans, which would involve all relevant stakeholders. This would be organised via the financial support in WP2009 of DG JLS Programme on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks". Member States and stakeholders would, where appropriate, build upon the ENISA "CSIRT Exercise book" and the exercises planned by ENISA in 2009.
Operational objective 3.3 Reinforcement of	**Action 3.3.1** The Commission would stimulate Member States to further develop and reinforce the pan-European

[92] See footnote 74.

operational co-operation and dialogue between National/Governmental CERTs	cooperation among well-functioning National/Governmental CERTs. To this end, existing organisations such as the European Governmental CERTs Group (EGC) could be leveraged. In addition, the Commission would ask ENISA to continue and augment its activities aimed at reinforcing the capabilities of CERTs in Europe as well as encouraging operational cooperation and dialogue amongst National/Governmental CERTs. The cooperation would also be reinforced by the step-wise development of a European Information Sharing and Alert Systems whose building blocks would be national information and alert sharing systems, for which National/Governmental CERTs are a key resource. These activities would also build upon the results of the study planned in Action 3.3.2, as well as on the results of the 2 prototype implementations of EISAS being funded under WP2008 of the Programme on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks" (DG JLS).
	Action 3.3.2 The Commission would launch a study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet. It is expected that the results of this study would also contribute to the reinforcement of operational co-operation and dialogue between National/Governmental CERTs.
Operational objective 3.4 Clarification of legal obstacles to the exchange of information on incidents and providing collaborative platforms for ensuring the confidentiality of information	**Action 3.4.1** The Commission would take the lead in promoting the discussion of workable frameworks to support the exchange of sensitive information. Such action could leverage the Public-Private Partnership planned in Action 1.2.1.
Operational objective 4.1 Defining EU priorities for Internet long term stability and resilience	**Action 4.1.1** The Commission would involve all relevant stakeholders in defining a set of European public policy priorities for Internet stability and resilience. To this end, the Commission would organise meetings and/or participate in relevant fora.
	Action 4.1.2 The Commission would strengthen its interaction with key European Internet Governance actors (i.e. CENTR and RIPE) in order to devise a common set of EU priorities for Internet stability and resilience.
	Action 4.1.3 The Commission would launch a study on DNS resilience in order to identify the main challenges to ensure the security and resilience of the global Domain Name System, one of the key critical infrastructures of the Internet. The study would be funded under the 2008 Programme on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks" (DG JLS). The results of this activity will be instrumental for the definition of EU priorities for Internet long term stability and resilience.
	Action 4.1.4 In the context of FP7 or other programmes the Commission would closely monitor the projects focused on Internet stability and resilience and use the results of such projects to define the EU priorities in the area under consideration.
Operational objective 4.2 Launching a European-led international initiative with the aim to create a set of principles for Internet security and resilience	**Action 4.2.1** The Commission would define a first proposal of a set of principles for Internet security and resilience. To this end, due account would be taken of existing initiatives and of the work of other relevant organisations (such as the OECD, ICANN, the Internet Governance Forum, ITU, etc).
	Action 4.2.2 The Commission would propose and take the lead in defining a roadmap for an international initiative aimed at creating a set of principles for Internet security and resilience. To this end, strategic cooperation with third countries will be developed, in particular with countries like USA, Canada and Japan, as a vehicle to build global consensus.

4.3. Option 3: the establishment of a binding framework

Under this policy option most of the issues listed above would be addressed through a number of binding measures at the European level. The Member States would then be subjected to certain general obligations, detailing minimum common-for-all requirements.

The binding measures would take the form of a Directive, a Regulation or a Decision.

The actions that would be put in place under policy option 3 are the following:

Operational objective 1.1 Enhancing the cooperation on policy areas that constitute the common ground of national approaches.	**Action 1** The Commission would propose binding measures to define a baseline that would harmonise national policies. Such measures may focus on additional security and resilience of CII (for instance, those that relate to obligations for mutual assistance, priority calls, emergency services, continuity of services for vital functions, etc.) that would be outside the framework of the market legislation already proposed (i.e. the review of the e-communication Regulatory Package).
Operational objective 1.2 Information sharing and exchange of good policy practices	
Operational objective 2.1 Knowledge sharing to deepen the understanding and mastering of challenges for the security and resilience of CII	**Action 2** The Commission would propose binding measures to define the role and responsibility of public and private stakeholders in security and resilience of CII for possible situations and scenarios.
Operational objective 2.2 Identification and dissemination of good baseline practices	
Operational objective 3.1 Identification and agreement on a minimum level of capabilities and services for well-functioning National/Governmental CERTs and the Establishment of well-functioning National/Governmental CERTs	**Action 3** The Commission would propose binding measures to improve operational preparedness. The first element would be a minimal set of standard for harmonised level functions and services for National/Governmental CERTs, with a view to make them contribute to a centrally organised European incident response capability. The second element would be a framework for national contingency planning with a view to develop EU wide contingency plans.
Operational objective 3.2 Development of Operational Contingency Plans and Performance of Exercises	
Operational objective 3.3 Reinforcement of operational co-operation and dialogue between National/Governmental CERTs	
Operational objective 3.4 Clarification of legal obstacles to the exchange of information on incidents and providing collaborative platforms for ensuring the confidentiality of information	
Operational objective 4.1 Defining EU priorities for Internet long term security and resilience	There is no possible short-term binding measure that can be taken for achieving operational objectives 4.1 and 4.2 – see sec. 5.5.
Operational objective 4.2 Launching a European-led international initiative with the aim to create a set of principles for Internet security and resilience	

5. ANALYSIS OF IMPACTS

This section of the report **analyses the impacts** associated with each of the clusters of policy priorities represented in the main policy options presented in Section 4, on the basis of the full tables of impacts which can be found in Annex 3.

5.1. The challenge of trustable data

Before proceeding to analyse the expected impacts of each option, it is necessary to point out that trustable data to base the analysis are not readily available. A full discussion of the underlying causes of this problem can be found in section 2.1.9.

5.2. Impacts indicators – magnitude and likelihood

For the assessment of each of the impacts two dimensions are analysed, magnitude and likelihood:

- the **magnitude** of each impact may be viewed as the level of influence a particular policy option would have on specific issues falling within the economic, environmental and social context. The magnitude is expressed using the following notation:

---	Extremely negative impact
--	Very negative impact
-	Negative impact
0	No impact at all, neither positive nor negative
+	Positive impact and positive contribution to achieving the specific objective
++	Very positive impact and clear contribution to achieving the specific objective
+++	Extremely positive and decisive impact and extremely clear positive contribution to achieving the specific objective

- the **likelihood** of an impact is understood as the likeliness that an impact would occur as a result of a proposed action, which is assumed to take place, taking into account the possibilities and limitations of that specific action (i.e. the lack of information on which to base the substantial contents of an action). The likelihood is expressed using the following notation:

0	No likelihood
1	Low likelihood
2	Medium likelihood
3	High likelihood

The total impact rating is calculated by multiplying the magnitude rating by the likelihood rating. For the baseline scenario, which is the basis for comparison of the options, all the ratings for magnitute and likelihood are set to 0.

This analysis will explore impacts on stakeholders in three different dimensions: **economic, social and environmental**. The following table outlines the main impact indicators that were considered:

Economic	**Social**	**Environmental**
Less costs for companies operating in more member States due to reduced differences in obligations concerning security and resilience	Increased networking between European / International experts including on social aspects of security and resilience Enhanced dialogue about social aspects of security and resilience	Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII;
Higher economies of scale in implementing security obligations for companies operating in more Member States	Equal levels of protection of EU citizens' personal data and privacy due to enhanced security of CII	Better use of energy for ICT due to better rationalisation of the security and resilience measures
Increased availability of information on challenges and risks for security and resilience	Better reaching out to citizens	Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures
Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual Member State	Higher citizens' trust in Information Society services and systems	
Efficient management due to better governance mechanisms	Better response to cyber attacks and cyber disruptions limiting the negative impacts on society	
Enhanced know-how	Better quality of services for citizens and SMEs of better quality due to lower level of disruptions	
Less costs of cyber attacks due to better preparedness and faster response	Better safeguarding of fundamental rights through enhancing protection of CII	
More investments triggered by common policy objectives and standards for security and resilience at EU level		
More users and use due to increased confidence		
More competitive SMEs due to better knowledge, more information and more support to tackle security risks		
Lower risks of catastrophic failures/accidents in Europe		
Lower operational risks for business due to higher level of security and resilience of CII		

Example: In order to illustrate the rationale behind the assigned ratings we could take as an example the following indicator: "Increased availability of information on challenges and risks for security and resilience". In the case of a non-binding framework it takes values of +++ for magnitude and 2 for likelihood, whereas for the binding framework the values are ++ and 1 respectively. This assessment is based on information from the consultation process accompanying the impact assessment which showed that experts in the field are willing to exchange information in non-formalised dialogue, based on trust and mutual collaboration. Binding measures would possibly limit the exchange of information only to what is strictly required and diminish the efficiency of the process.

Summary table of impacts						
Impacts	Business as usual		Implementation of measures within a non-binding framework		Establishment of a bin framework	
	Magnitude	Likelihood	Magnitude	Likelihood	Magnitude	Likelihoo
Economic						
Less costs for companies operating in more MSs due to reduced differences in obligations concerning security and resilience	0	0	+++	2	++	2
Economies of scale in implementing security obligations for companies operating in more MSs	0	0	+++	3	+++	2
Enhanced know-how	0	0	++	2	++	1
More investments triggered by common policy objectives and standards for security and resilience at EU level	0	0	+++	2	++	1
More users and use due to increased confidence	0	0	++	2	+	2
Lower operational risks for business due to higher level of security and resilience of CII	0	0	+++	3	++	2
Increased availability of information on challenges and risks for security and resilience	0	0	+++	2	++	1
Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual MS	0	0	+++	3	+	2
Efficient management due to better governance mechanisms	0	0	+++	3	++	2
Lower risks of catastrophic failures/accidents in Europe	0	0	+++	3	++	2
Less costs of cyber attacks due to better preparedness and faster response	0	0	+++	3	++	2
More competitive SMEs due to better knowledge, more information and more support to tackle security risks	0	0	++	2	++	2
Social						
Increased networking between European/International experts including on social aspects of security and resilience	0	0	++	2	+	1
Enhanced dialogue about social aspects of security and resilience	0	0	++	2	+	1
Equal levels of protection of EU citizens' personal data and privacy due to enhanced security of CII	0	0	+++	2	++	2
Higher citizens' trust in Information Society services and systems	0	0	++	1	++	1
Better safeguarding of fundamental rights through enhancing protection of CII	0	0	++	2	+	2
Better response to cyber attacks and cyber disruptions limiting the negative impacts on society	0	0	+++	3	++	2
Better reaching out citizens	0	0	+++	2	++	1
Better quality of services to citizens and SMEs of better quality due to lower level of disruptions	0	0	+++	1	+++	1
Environmental						
Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	0	0	+	1	+	1
Better use of energy for ICT due to better rationalisation of the security and resilience measures	0	0	++	2	++	1
Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	0	0	++	2	++	1

5.3. Option 1 (business as usual): analysis of impacts

As explained in the baseline scenario, the choice of policy option 1 (business as usual) would lead to a **generally unsatisfactory result** across all specific objectives. This is a direct consequence of the **inherent nature and characteristics of the problems** that were discussed above. In particular, the need for a European-wide approach to the security and resilience of CII would hardly be met by failing to provide some form of framework/platform for coordination.

In fact, Member States have had until now different approaches or have not yet developed a holistic policy approach to security and resilience of CII. Without Community actions to steer the cooperation at European level, **Member States would continue interacting and communicating on bilateral or regional level only**. This may lead to the development of policies for security and resilience mostly based just on national experience, with limited use of good policy practices, and at different paces. As a result **Member States' national policies for security and resilience of CII would remain fragmented** and, due to the global dimension of the threats and risks, might turn out to be ineffective for Europe at large, in particular with respect to protecting fundamental rights and, above all, privacy.

Moreover, **information sharing between private and public sector organisations would not develop at European level** due to the lack of an appropriate governance model. Member States would continue developing their own national arrangements with multiplying costs for the private sector. This may **hinder the process of creating a common understanding about the risks, threats and vulnerabilities** faced by the stakeholders. In addition, uncoordinated national measures might increase the risk of fragmentation, systemic gaps and incompatibilities.

Commission funded **studies and research projects** collecting and disseminating information on the economic impacts of security incidents, as well as more fundamental research on security challenges **would continue** to deliver important findings and results; however, **their actual value might be undermined** by the lack of a mechanism to address these issues in a **European and global perspective**.

In addition, as not all Member States would have established well-functioning National/Governmental CERTs, **pan-European cooperation would be limited to informal and ad hoc cooperation**. The experience and value of existing structures such as the European Governmental CERTs Group (EGC) would remain limited only to those few Member States whose National/Governmental CERTs qualify for participation. **Legal obstacles would continue to be a major concern** for stakeholders with respect to exchange of sensitive information. If no action is undertaken to design appropriate frameworks and procedural standards for information exchange the progress would be very limited.

Last, not least, **Member States would continue having different and diverse priorities for Internet security and resilience**. Member States would continue struggling in their attempt to protect on their own the good functioning of their "domestic" Internet in an operational and technological environment that is global by its very nature. Even worse, without a coordinated approach to define European priorities for Internet security and resilience, priorities in this field might be set by other countries at the international level where individual Member States would not be in a strong position to influence decisions – and therefore **unable to promote core European values, such as privacy and data protection, in the most efficient and effective way**.

5.4. Option 2 (non-binding framework): analysis of impacts

As can be seen from the tables in Section 5.2 and in Annex 3, the choice of policy option 2 (creation of a non-binding framework) would lead generally to good results across all specific objectives, in a timeframe that corresponds to the need to act as rapidly as possible, while fully respecting national competences.

In particular, the use of a non-binding approach – providing tools and frameworks, raising awareness amongst stakeholders, encouraging dialogue and analysis of 'lessons learnt' and in general making sure that **existing and prospective activities would move toward a full European dimension** – would ensure that two key elements to achieve the objectives of this policy proposal are fully taken into account. First of all, that a **full-fledged exchange of**

information between all the stakeholders takes place. Secondly, that the potential subjects of the measures under consideration have a chance to **fully participate** in the definition of their key aspects.

The first element is important because at present the quantity and quality of available information on many fundamental aspects of the environment under consideration are **not completely satisfactory** (e.g. on the economic impact of security incidents).

A non-binding approach would rapidly allow all stakeholders to engage in a **stock-taking exercise** which would usefully contribute to a proper understanding of which substantive content should the proposed measures take over time.

The second element is also relevant, because when considering policies related to the security and resilience of CII, the sheer number of stakeholders from different sectors and from each Member State, each with different sensitivities, goals, responsibilities and expectations, makes it essential to **avoid "top-down" approaches** that would unavoidably deprive the planned measures of a large part of their efficacy and lead to loss of time.

A lack of proper discussion with the expected 'targets' of such measures might result in a compliance that would only be formalistic.

For almost all impact dimensions, therefore, the **likelihood indicator is rather high**: it is expected that a non-binding approach would be highly conducive to stock-taking, information gathering and exchange of good practices, and would be well received by stakeholders, which could substantially contribute to the strategic and operational elements of the overall strategy, providing timely responses.

In addition, for those impact indicators that are **mostly focused on information sharing** (exchange of good practices, reaching out to citizens and other societal groups, intensifying networking between professionals) option 2 would have a rather high magnitude, as this **kind of activities are by their nature well suited to a non-binding approach** without "top-down" impositions.

Moreover, the ensemble of the measures would have a rather positive impact on the protection of fundamental rights, in particular privacy, due to both the enhanced level of security as well as the more thorough discussion that would take place between public and private sector on the societal aspects of security and resilience of CII.

Finally, a Communication from the Commission to the European Parliament and the Council could be rapidly adopted and enable concrete progress to be made in a timely manner, while allowing the full involvement of the Parliament and the Council in the debate (e.g. through Council Conclusions or Resolutions or Parliamentary Reports).

5.5. Option 3 (binding framework): analysis of impacts

As can be seen from the tables in Section 5.2 and in Annex 3, the choice of policy option 3 (creation of a binding framework) would lead generally to good results across almost all specific objectives. Nevertheless, this statement must be **qualified** in two important ways.

First of all, it can be seen from the tables that the **likelihood indicator of the analysed impacts is often at a rather low level**. This is a direct consequence of the way in which this indicator was defined, i.e. as the "likeliness that an impact would occur as a result of a proposed action, which is assumed to take place, taking into account the possibilities and limitations of that specific action".

In the context of option 3, this should be understood as referring to the foreseeable **difficulty** for any binding measure (a Directive, a Regulation or a Decision) to be as **specific** and **fact-based** as needed in order to achieve the planned objective.

The complexity of this field requires a long process of **stock-taking** and **dialogue** to understand how the **substantial content** of a binding instrument should be framed. The risk, in this context, is to enact binding measures that would be formally correct but practically irrelevant, if not counterproductive.

Secondly, specific objective #4 (the enhancement and resilience of the Internet) can be **hardly** addressed through a binding measure, at least in the short- and medium-term. This is due to the fact that an international binding instrument defining the basic principles and rules for enhancing the security and resilience of the Internet could be negotiated only on the basis of a recommendation by the Commission to the Council to authorise the former to conduct the necessary negotiations.

Besides the fact that such a Recommendation could not, as a matter of fact, be considered as a binding instrument *per se* (rather as the very first step possibly leading to the definition and enactment of a binding measure) a brief analysis of the international situation suggests that at the moment there are not the **political conditions** for starting the process without a proper stock-taking exercise or preliminary negotiations at the international level having taken place.

Moreover, the use of binding measures might be ineffective, if not damaging, for those activities that are **mostly focused on information sharing**, such as the exchange of good practices, reaching out to citizens and various societal groups, augmenting networking between professionals.

These activities, with some very limited exceptions (e.g. mandatory disclosure of security breaches, **which has in fact already been proposed in the context of the reform of the Electronic Communications package**) are not well suited to 'top down' approaches.

Finally, a binding measure would take too much time to produce concrete effects. All such measures (directives, regulations, decisions) would be subject to the co-decision procedure and, in case of a directive, to an additional eighteen to twenty-four months for transposition into national law. In this respect, it should be mentioned that a Directive relevant to the objectives of this policy proposal – the Directive on the Identification of European Critical Infrastructures – is already in the pipeline, but has not been adopted after more than two years of negotiation. It is difficult to see how a binding instrument for the policy discussed here would take less time to be adopted.

6. COMPARING THE OPTIONS

On the basis of the discussions conducted in the previous sections and of the tables in Annex 3 it seems that **policy option 2 turns out to be the best to achieve the objectives of the proposed policy**.

First of all, **policy option 1 should be discarded**: continuing with "business as usual", in fact, would produce a number of negative consequences that would have an adversely impact across all dimensions, as discussed in section 5.3.

The choice is therefore between a non-binding and a binding framework – policy option 2 versus policy option 3.

A mere reading of the indicators would indicate that **policy option 2 would be preferable** *per se*.

However – considering also that, due to the lack of reliable data, the assessment of the impacts was conducted substantially on the basis of experience, of the results of consultations and on proxy evaluations – the **political dimension** of the choice between the two policy options, as well as the possible **timing** of an action *vis-à-vis* the need to act rapidly, should be duly taken into account.

Regarding the **political dimension**, during the consultation process that informed this impact assessment (as well as the one carried out for the EPCIP Directive) Member States and the industry seemed to **oppose the option of binding approaches** for a variety of reasons, some of which were already discussed in section 5.5.

It is worth stressing that ensuring security and resilience of CII requires cooperation among public and private actors. Reality shows that efficient cooperation is largely based on trust and interpersonal relations among experts in the security field.

Trust and credibility are intangible assets which cannot be created through binding measures. Although the latter can oblige the actors to comply with certain duties, cooperation risks remaining limited only to what is strictly required and, even in those cases, to be more formalistic than effective. Considering the high degree of 'information asymmetry' in this area – with the private sector having often a major control over data that is needed for policy decisions – binding approaches might **backfire**, by producing a **mere formal compliance** by the stakeholders but very few practical effects (if any).

On the contrary, a non-binding approach, while not forcing compulsory measures, would be more beneficial at this stage in steering a dialogue through which interested parties can work out the most efficient way to cooperate and share best practices. In addition, as pointed out by some of the stakeholders during the consultation process, introducing regulatory measures would divert the focus from cooperation among technical experts on operational issues towards pure discussion of legal matters. In fact, during the consultation process Member States' and private sector representatives expressed strong support for the proposed initiative and confirmed the need and willingness to cooperate at EU level, as long as such cooperation was not forced upon them

Last, not least, a purely regulatory approach is advisable when dealing with strategic, mid- to long-term public policy approaches; but the **speed of technological development** and the resulting fluidity of operational requirements makes binding approaches potentially ill suited to produce practical effects for enhancing the security and resilience of CII.

This last consideration is directly connected to the **timing** of any proposed instrument. As discussed above, a Communication, as opposed to a binding instrument such as a Directive, a Regulation or a Decision, could be **adopted quickly** and enable stakeholders to start **working rapidly**.

This **does not mean** that binding approaches do not have a place when trying to enhance the level of security and resilience of CII: to the contrary, the proposals by the European Commission to reform the Electronic Communication regulatory package – in particular the amendments to art. 13 of the Framework Directive, which includes provisions to strengthen operators' obligations to ensure that appropriate security and integrity measures are taken to meet identified

risks and to guarantee the continuity of supply of services, as well as provisions on mandatory breach notification – are a proof that, **wherever feasible and useful**, this path was taken.

In conclusion, this report suggests that **policy option 2 is preferable in the short- and medium-term**. Once the actions proposed in this report are launched and a proper stock-taking exercise on their results has taken place – including the results of the **public consultation on the future of network and information security**, running from 7 November 2008 until 9 January 2009 – then there would be the basis for a more thorough analysis of the substantial content of any binding measures. At that point in time, it **might be possible** to recommend the implementation of actions similar to those elaborated in policy option 3. This would not necessarily mean that the "non-binding" approach suggested in policy option 2 would be abandoned, as some activities – mostly related to nurturing cooperation, as discussed above – would continue not to be easily framed in terms of binding measures. This opens the possibility, to be assessed after the stock-taking exercise, for a combination of binding and non-binding measures.

7. MONITORING AND EVALUATION

7.1. What are the core indicators of progress towards meeting the objectives?

The progress on this initiative would be monitored by Commission Services.

The following list of indicators could be used to monitor the achievement of each specific objective:

Specific objective 1: Bridging gaps in national policies for the security and resilience of CII	Number of meetings and conferences organised at EU level with relevance to security and resilience of CII
	Number of instances of pan-European information sharing activities
	Reduced divergence of Member States' approaches to security and resilience
Specific objective 2: Enhancing the European governance for the security and resilience of CII	Existence of a well-functioning PPP
	Number of European agreements on mutual assistance, recovery, and remedial strategies
	Number of conferences/meetings at European level involving public and private stakeholders
	Number of good public policy practices for security and resilience identified at European level
	Number of identified good operational practices for industrial deployment
	Number of vulnerabilities disclosures
	Agreement on methodology for risk assessment
	Agreement on common terminology and procedures for the collection and dissemination of information on economic impacts of security incidents
	Number of studies/research projects aimed at identifying challenges (and possible solutions) to enhance security and resilience
	Number and quality of frameworks and practices to support the exchange of sensitive information
Specific objective 3: Strengthening Europe's operational incident response capability	Number of well-functioning National/Governmental CERTs
	Number of National/Governmental CERTs participating in the European Governmental CERTs Group
	Number of Member States having developed operational contingency plans
	Number of Member States having national information and alert systems to reach out to citizens and SMEs
	Number of conferences/meetings for exchange of experience and good practices
	Number of pan-European exercises to test contingency plans
	Development of a European information sharing and alert system
	Number and actual usage of frameworks for exchange of sensitive information
Specific objective 4: Enhancing Internet security and resilience	Agreement on a set of European public policy priorities for Internet stability and resilience
	Number of conferences/meetings in which EU Member States defend commonly agreed goals
	Number of international agreements on mutual assistance, recovery, and remedial strategies
	Number of meetings between European/International experts

7.2. Broad outline of possible monitoring and evaluation arrangements

Firstly, the Commission could follow-up the development of the studies[93] related to:

measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet ;

the definition of criteria for European critical infrastructures for the ICT sector.

The Commission could also follow-up the development of the prototyping activity for EISAS. Currently, two projects with the participation of some Member States are being funded under the DG JLS Work Programme 2008 on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks". These two projects are complementary in that the first one covers aspects of horizontal integrations (cooperation between national systems) and the second one focuses on vertical integration (federating systems on a national level). Both perspectives have indeed to be investigated to realise a proof of concept for the future development of EISAS. Regular stock takings of such activities would be done until the end of 2010.

Secondly, the Commission could promote and monitor the uptake of specific guidelines and products on security and resilience being produced by ENISA, such as the good practices for National/Governmental CERTs, the exercise collection for CERTs, the resilience good practices, etc.

Thirdly, the Commission could launch and follow-up new projects on pan-European contingency planning under the DG JLS Work Programme 2009 on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks". It would monitor the development of the cooperation between National/Governmental CERTs and would take stock at the beginning of 2011.

Fourthly, the Commission could monitor the work of the project on a Task Force for DNS resiliency that is being launched under the DG JLS Work Programme 2008 on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks".

Fifthly, the Commission could continue to contribute to and benefit from the debate on a modernised Network and Information Security policy at EU level that will take place between now and 2010, when a proposal on the future of Network and Information Security will be made. This debate would provide input on the challenges and priorities for network and information security and the instruments needed at EU level to tackle these challenges, on the possible EU instruments or actions to reinforce incident response capability, on the instruments to foster international dialogue and cooperation for Internet security and resilience.

Last but not least, the Action Plan, being part of the Communication, would provide the milestone indicators for measuring the progress and the achievement of the objectives of the initiative.

[93] Funded under DG JLS Work Programme 2008 on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks".

ANNEXES 1-19

ANNEX 1: ORGANISATION AND TIMING

Period/Activity	**Jan 2007**	**Apr 2007**	**Jun 2007**	**Sep 2007**	**Dec 2007**	**Jan 2008**	**Feb 2008**	**Apr 2008**	**May 2008**	**Jun 2008**	**July 2008**	**Aug 2008**	**Sep 2008**	**Oct 2008**	**Nov 2008**	**Dec 2008**	**Q1 2009**
CONSULTATION PROCESS:																	
Informal meeting with MSs' experts																	
Call for comments on the ARECI report																	
Second meeting with MSs																	
Workshop on business continuity of ccTLDs																	
Public consultation on an EU Strategy for International Co-operation on ICT																	
Workshop on lessons learnt from recent large scale attacks						17th											
Meetings with MSs for stock-taking on national initiatives and criteria definition and to discuss the process of defining sectoral criteria to identify critical infrastructures in the ICT sector (Questionnaire sent to MSs to take stock of national CIIP initiatives and processes to define ICT criteria)							5th		29th								
Thematic workshop on the role of the private sector in the CIIP Initiative										26th							
INTER-SERVICE STEERING GROUP:					14th									20th	4th		
IA STUDY (The process of preparing the IA will be assisted by an external contractor):																	
1st (kick-off) meeting with the contractor								3rd									
Report on the proposed policy options and an initial assessment									22nd								
2nd meeting to present report on policy option proposals													1st				
Draft final report														6th			
Final Report submitted by the contractor														24th			
Final IA report to be sent to IAB															26th		
IAB opinion																17th	
Inter-service consultation with IA report, executive summary and citizen's summary																	
Submission of the draft proposal + IA summary to DGT																	
Adoption by the Commission																	

ANNEX 2: SUMMARY OF THE POLICY OPTIONS

Option 1 - Business as usual

Specific Objectives	Business as usual
1. Bridging gaps on national CIIP policies across Europe	To date, MSs have different approaches or have not yet developed a holistic policy approach to security and resilience of CII. In addition, the National policy approaches have varying focus and breadth. Without Community actions to steer the cooperation at European level, MSs would continue interacting and communicating on bilateral or regional level only. This may lead to the development of policies for security and resilience mostly based just on National experience, with limited use of policy good practice, and at their own pace. As a result MSs' national policies for security and resilience of CII would likely continue to be fragmented and, due to the global dimension of the threats and risks, might turn out to be ineffective for Europe at large. Given the lack of a pan-European mechanism, the information sharing and the exchange of good policy practices and standards would be very limited, besides regional and ad hoc cooperation. The information sharing and the exchange of good policy practices and standards would remain limited mostly to technical and/or operational aspects addressed via ad hoc schemes and /or by organisations (such as ENISA). And, the public policy perspective of security and resilience would remain undeveloped and, therefore, not be properly addressed at European level.
2. Enhancing CIIP governance across the EU	Information sharing between private and public sector organisations would not develop at European level due to the lack of an appropriate governance model. MSs would continue developing their own national arrangements with multiplying costs for the private sector. This may hinder the process of creating a common understanding about the risks, threats and vulnerabilities faced by the stakeholders. In addition, uncoordinated National measures might increase the risk of fragmentation, systemic gaps and incompatibility. Commission funded studies and research projects (under FP7) in the area of collection and dissemination of information on the economic impacts of security incidents (i.e. the study on the economic implications of the security and resilience of CII is already planned for 2009, under the eCommunications budget line) would continue to deliver important findings and results. However, their actual value might be undermined by the lack of a mechanism to address these issues in a European and global perspective. In the context of FP7 or other programmes, the Commission would launch calls for research projects aimed at identifying prospective challenges and develop the necessary technologies to enhance the security and resilience of CII. However, the findings of such projects would remain of little value if no follow-up action is taken at the EU level.
3. Strengthening Europe's incident	The importance of having National/Governmental CERTs with appropriate level of resources, skills, knowledge, operational and services capability would continue to be regarded differently in different MSs. Thus, there will be no basis to ensure strong national incident response capabilities, which is a pre-condition

Specific Objectives	Business as usual
response capability	for effective pan-European cooperation. To date only few MSs have started developing contingency plans. The development of operational contingency plans would not be considered as an outmost priority by all MSs. There might be no sufficient preparedness at national level to cope with and limit the impact of cyber accidents and disruptions. The exchange of good practices and methodological standards would be limited, leading to very limited capability to develop European-wide operational contingency plans. As not all MSs would have established well-functioning National/Governmental CERTs, pan-European cooperation would be limited to informal and ad hoc cooperation. The experience and value of existing structures such as the European Governmental CERTs Group (EGC) would remain limited only to those few MSs whose National/Governmental CERTs qualify for participation. Legal obstacles would continue to be a major concern for stakeholders with respect to exchange of sensitive information. If no action is undertaken to design appropriate frameworks and procedural standards for information exchange the progress would be very limited.
4. Enhancing Internet security and resilience	MSs would continue having different and diverse priorities for Internet security and resilience. In addition, some MSs would continue not giving proper policy relevance to the security of the Internet. MSs would continue struggling in their attempt to protect on their own the good functioning of their "domestic" Internet in an operational and technological environment that is global by its very nature. If MSs do not act together and take the lead to define European priorities for Internet security and resilience, priorities might be set by other countries at the international level where individual MSs would not be in a strong position to influence decisions.

Option 2 - Implementation of measures within a non-binding framework

Specific Objectives	Implementation of measures within a non-binding framework
1. Bridging gaps on national CIIP policies across Europe	The Commission would work with Member States in identifying transferable examples of public policy practices and commonalities. Such activity would benefit from stock-taking and analysis of existing commonalities, building upon existing studies and analysis. The Commission would establish a European Forum for Member States to share information and good policy practice on security and resilience for CII. The activity would benefit from the result of the work and operational activities conducted by other organisations (e.g. ENISA).
2. Enhancing CIIP governance across the EU	The Commission would establish a European Public-Private Partnership, to support cooperation and information sharing on European and global challenges for the security and resilience of CII. The primary focus would be on the European dimension of the challenges for security resilience of CII, both from a strategic (e.g. good practices for public policy) and tactical/operational (e.g. industrial deployment) perspective. To this end, the PPP would build upon and complement both existing national initiatives as well as the operational work conducted by ENISA.

Specific Objectives	Implementation of measures within a non-binding framework
	The Commission would establish a European Public-Private Partnership, to support cooperation and information sharing on European and global challenges for the security and resilience of CII. The primary focus would be on the European dimension of the challenges for security resilience of CII, both from a strategic (e.g. good practices for public policy) and tactical/operational (e.g. industrial deployment) perspective. To this end, the PPP would build upon and complement both existing national initiatives as well as the operational work conducted by ENISA. Topics to be discussed in the context of such partnership may include: - processes for vulnerability disclosure - practices for threat identification - methodologies for risk assessment - common terminology and procedures for the collection and dissemination of information on economic impacts of security incidents - workable frameworks and practices to support the exchange of sensitive information. The Commission would analyse the methodological and legal challenges related to the collection and dissemination of information on the economic impacts of security incidents. To this end, a study on the economic implications of the security and resilience of CII should be launched in 2009, under the eCommunications budget line. The results of these activities would feed into the work of the European partnership. In the context of FP7 or other programmes, the Commission would launch, where appropriate, calls for research projects aimed at identifying prospective challenges (and possible solutions) to enhance the security and resilience of CII.
3. Strengthening Europe's incident response capability	The Commission would work with Member States on defining the appropriate baseline of capabilities, services and operational functions for National/Governmental CERTs. The definition and a wide adoption of such a baseline would reinforce the national response capability and ensure that national capabilities could cooperate at the European and international levels. The Commission would encourage and support (inter alia by promoting good practices and guidelines) Member States to establish well-functioning National/Governmental CERTs with the aim to integrate their function/operation more in a public policy dimension. In addition to their operational function, National/Governmental CERTs could play the role of catalysers of stakeholder interests and capabilities for public policy activities, including those related to establishing national information and alert sharing systems to reach out to citizens and SMEs, which constitute the national building blocks for EISAS. The activity would benefit from the work conducted by ENISA in the context of its CERT-related activities. The Commission would stimulate and support Member States in developing national operational contingency plans for CII. To this end, the Commission would organise meetings / conferences to exchange experience, lessons learnt and 'good practices'. The establishment of national contingency plans would be instrumental for stronger cooperation and coordination towards European-wide operational contingency plan. This activity would also be supported via the forum planned in Action 1.2.1, where common strategic objectives could be discussed. ENISA could

Specific Objectives	Implementation of measures within a non-binding framework
	be asked to support these exchanges by providing its expertise on the operational dimension of this challenge. The Commission would facilitate the Member States to design and perform pan-European exercises to test contingency plans, which would involve all relevant stakeholders. This would be organised via the financial support in WP2009 of DG JLS Programme on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks". Member States and stakeholders would, where appropriate, build upon the ENISA "CSIRT Exercise book" and the exercises planned by ENISA in 2009. The Commission would stimulate Member States to further develop and reinforce the pan-European cooperation among well-functioning National/Governmental CERTs. To this end, existing organisations such as the European Governmental CERTs Group (EGC) could be leveraged. In addition, the Commission would ask ENISA to continue and augment its activities aimed at reinforcing the capabilities of CERTs in Europe as well as encouraging operational cooperation and dialogue amongst National/Governmental CERTs. The cooperation would also be reinforced by the step-wise development of a European Information Sharing and Alert Systems whose building blocks would be national information and alert sharing systems, for which National/Governmental CERTs are a key resource. These activities would also build upon the results of the study planned in Action 3.3.2, as well as on the results of the 2 prototype implementations of EISAS being funded under WP2008 of the Programme on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks" (DG JLS). The Commission would launch a study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet. It is expected that the results of this study would also contribute to the reinforcement of operational co-operation and dialogue between National/Governmental CERTs. The Commission would take the lead in promoting the discussion of workable frameworks to support the exchange of sensitive information. Such action could leverage the Public-Private Partnership.
4. Enhancing Internet security and resilience	The Commission would involve all relevant stakeholders in defining a set of European public policy priorities for Internet stability and resilience. To this end, the Commission would organise meetings and/or participate in relevant fora. The Commission would strengthen its interaction with key European Internet Governance actors (i.e. CENTR and RIPE) in order to devise a common set of EU priorities for Internet stability and resilience. The Commission would launch a study on DNS resilience in order to identify the main challenges to ensure the security and resilience of the global Domain Name System, one of the key critical infrastructures of the Internet. The study would be funded under the 2008 Programme on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks" (DG JLS). The results of this activity will be instrumental for the definition of EU priorities for Internet long term stability and resilience. In the context of FP7 or other programmes the Commission would closely monitor the projects focused on Internet stability and resilience and use the results of such

Specific Objectives	Implementation of measures within a non-binding framework
	projects to define the EU priorities in the area under consideration. The Commission would define a first proposal of a set of principles for Internet security and resilience. To this end, due account would be taken of existing initiatives and of the work of other relevant organisations (such as the OECD, ICANN, the Internet Governance Forum, ITU, etc). The Commission would propose and take the lead in defining a roadmap for an international initiative aimed at creating a set of principles for Internet security and resilience. To this end, strategic cooperation with third countries will be developed, in particular with countries like USA, Canada and Japan, as a vehicle to build global consensus.

Option 3 - Establishment of a binding framework

Specific Objectives	Establishment of a binding framework
1. Bridging gaps on national CIIP policies across Europe	The Commission would propose binding measures to define a baseline that would harmonise national policies. Such measures may focus on additional security and resilience of CII (for instance, those that relate to obligations for mutual assistance, priority calls, emergency services, continuity of services for vital functions, etc.) that would be outside the framework of the market legislation already proposed (i.e. the review of the e-communication Regulatory Package).
2. Enhancing CIIP governance across the EU	The Commission would propose binding measures to define the role and responsibility of public and private stakeholders in security and resilience of CII for possible situations and scenarios.
3. Strengthening Europe's incident response capability	The Commission would propose binding measures to improve operational preparedness. The first element would be a minimal set of standard for harmonised level functions and services for National/Governmental CERTs, with a view to make them contribute to a centrally organised European incident response capability. The second element would be a framework for national contingency planning with a view to develop EU wide contingency plans.
4. Enhancing Internet security and resilience	There is no possible short-term binding measure that can be taken for achieving operational objectives 4.1 and 4.2 – see sec. 5.5

ANNEX 3: TABLE OF IMPACTS

Option 1: Business as usual

Objective	Likely development	Impact	Magnitude	Likelihood	Total
Specific objective 1: Bridging gaps on national policies for the security and resilience of CII (Option 1)					
Operational objective 1.1 Enhancing the cooperation on policy areas that constitute the common ground of national approaches.	To date, MSs have different approaches or have not yet developed a holistic policy approach to security and resilience of CII. In addition, the National policy approaches have varying focus and breadth. Without Community actions to steer the cooperation at European level, MSs would continue interacting and communicating on bilateral or regional level only. This may lead to the development of policies for security and resilience mostly based just on National experience, with limited use of policy good practice, and at their own pace. As a result MSs' national policies for security and resilience of CII would likely continue to be fragmented and, due to the global dimension of the threats and risks, might turn out to be ineffective for Europe at large.	**Economic**			
		Less costs for companies operating in more MSs due to reduced differences in obligations concerning security and resilience	---	1	---
		Economies of scale in implementing security obligations for companies operating in more MSs	---	2	------
		Enhanced know-how	0	0	**0**
		More investments triggered by common policy objectives and standards for security and resilience at EU level	--	2	----
		More users and use due to increased confidence	-	1	-
		Lower operational risks for business due to higher level of security and resilience of CII	--	2	----
		Social			
		Increased networking between European / International experts	0	0	**0**
Operational objective 1.2 Information sharing and exchange of good policy practices	Given the lack of a pan-European mechanism, the information sharing and the exchange of good policy practices and standards would be very limited, besides regional and ad hoc cooperation. The information sharing and the exchange of good policy practices and standards would remain limited mostly to technical and/or operational aspects addressed via ad hoc schemes and /or by organisations (such as ENISA). And, the public policy perspective of security and resilience would remain undeveloped and, therefore, not be properly addressed at European level.	Enhanced dialogue about social aspects of security and resilience	0	0	**0**
		Equal levels of protection of EU citizens' personal data and privacy due to enhanced security of CII	--	2	----
		Higher citizens' trust in Information Society services and systems	-	1	-
		Better safeguarding of fundamental rights through enhancing protection of CII	0	0	**0**
		Environmental			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	0	0	**0**
		Better use of energy for ICT due to better rationalisation of the security and resilience measures	-	1	-
		Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	-	1	-

Objective	Likely development	Impact	Magnitude	Likelihood	Total
Specific objective 2: Enhancing the European governance for the security and resilience of CII (Option 1)					
Operational objective 2.1 Knowledge sharing to deepen the understanding of challenges for the security and resilience of CII	Information sharing between private and public sector organisations would not develop at European level due to the lack of an appropriate governance model. MSs would continue developing their own national arrangements with multiplying costs for the private sector. This may hinder the process of creating a common understanding about the risks, threats and vulnerabilities faced by the stakeholders. In addition, uncoordinated National measures might increase the risk of fragmentation, systemic gaps and incompatibility. Commission funded studies and research projects (under FP7) in the area of collection and dissemination of information on the economic impacts of security incidents (i.e. the study on the economic implications of the security and resilience of CII is already planned for 2009, under the eCommunications budget line) would continue to deliver important findings and results. However, their actual value might be undermined by the lack of a mechanism to address these issues in a European and global perspective.	**Economic**			
		Increased availability of information on challenges and risks for security and resilience	-	1	-
		Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual MS	--	2	----
		Efficient management due to better governance mechanisms	--	2	----
		Enhanced know-how	0	0	**0**
		More investments triggered by common policy objectives and standards for security and resilience at EU level	-	2	--
		Lower risks of catastrophic failures/accidents in Europe	--	2	----
		Lower operational risks for business due to higher level of security and resilience of CII	--	2	----
		Social			
		Increased networking between European/ International experts	-	2	--
Operational objective 2.2 Identification and dissemination of good practices	In the context of FP7 or other programmes, the Commission would launch calls for research projects aimed at identifying prospective challenges and develop the necessary technologies to enhance the security and resilience of CII. However, the findings of such projects would remain of little value if no follow-up action is taken at the EU level.	Enhanced dialogue about social aspects of security and resilience	0	0	**0**
		Better response to cyber attacks and cyber disruptions	--	2	----
		Better safeguarding of fundamental rights through enhancing protection of CII	0	0	**0**
		Environmental			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	0	0	**0**
		Better use of energy for ICT due to better rationalisation of the security and resilience measures	--	1	--
		Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	--	1	--

Objective	Likely development	Impact	Magnitude	Likelihood	Total
Specific objective 3: Strengthening Europe's operational incident response capability (Option 1)					
Operational objective 3.1 The identification and agreement on a minimum level of capabilities and services for well-functioning National/Governmental CERTs and the establishment of well-functioning National/ Governmental CSIRT	The importance of having National/ Governmental CERTs with appropriate level of resources, skills, knowledge, operational and services capability would continue to be regarded differently in different MSs. Thus, there will be no basis to ensure strong national incident response capabilities, which is a pre-condition for effective pan-European cooperation.	**Economic**			
		Increased availability of information on challenges and risks for security and resilience	--	1	--
		Enhanced operational know-how	--	1	--
		Less costs of cyber attacks due to better preparedness and faster response	--	2	----
		More users and use due to increased confidence	-	1	-
Operational objective 3.2 Development of Operational Contingency Plans and Performance of Exercises	To date only few MSs have started developing contingency plans. The development of operational contingency plans would not be considered as an outmost priority by all MSs. There might be no sufficient preparedness at national level to cope with and limit the impact of cyber accidents and disruptions. The exchange of good practices and methodological standards would be limited, leading to very limited capability to develop European-wide operational contingency plans.	More competitive SMEs due to better knowledge, more information and more support to tackle security risks	--	2	----
		Lower risks of catastrophic failures/accidents in Europe	--	2	----
		Lower operational risks for business due to higher level of security and resilience of CII	--	2	----
		Social			
		Increased networking between European/ International experts	0	0	**0**
Operational objective 3.3 reinforcement of operational co-operation and dialogue between National/Governmental CERTs/CSIRTs	As not all MSs would have established well-functioning National/Governmental CERTs, pan-European cooperation would be limited to informal and ad hoc cooperation. The experience and value of existing structures such as the European Governmental CERTs Group (EGC) would remain limited only to those few MSs whose National/Governmental CERTs qualify for participation.	Equal levels of protection of EU citizens' personal data and privacy due to enhanced security of CII	-	1	-
		Better reaching out citizens	-	1	-
		Better response to cyber attacks and cyber disruptions	--	2	----
		Better quality of services to citizens and SME's of better quality due to lower level of disruptions	--	1	--
		Higher citizens' trust in Information Society services and systems	-	1	-
Operational objective 3.4 clarification of legal obstacles to the exchange of information on incidents and providing collaborative platforms for ensuring the confidentiality of information	Legal obstacles would continue to be a major concern for stakeholders with respect to exchange of sensitive information. If no action is undertaken to design appropriate frameworks and procedural standards for information exchange the progress would be very limited.	**Environmental**			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	0	0	**0**
		Better use of energy for ICT due to better rationalisation of the security and resilience measures	-	1	-
		Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	-	1	-

Objective	Likely development	Impact	Magnitude	Likelihood	Total
Specific objective 4: Enhancing Internet security and resilience (Option 1)					
Operational objective 4.1 Defining EU priorities for Internet long term security and resilience	MSs would continue having different and diverse priorities for Internet security and resilience. In addition, some MSs would continue not giving proper policy relevance to the security of the Internet. MSs would continue struggling in their attempt to protect on their own the good functioning of their "domestic" Internet in an operational and technological environment that is global by its very nature.	**Economic**			
		Increased availability of information on challenges and risks for security and resilience	-	1	-
		Efficient management due to better governance mechanisms	--	2	----
		Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual MS	--	2	----
		Enhanced know-how	0	0	**0**
		More users and use due to increased confidence	-	1	-
		Less costs of cyber attacks due to better preparedness and faster response	--	2	----
		Lower risks of catastrophic failures/accidents in Europe	--	2	----
		Social			
Operational objective 4.2 Launching a European-led international initiative with aim to create a set of principles for Internet security and resilience	If MSs do not act together and take the lead to define European priorities for Internet security and resilience, priorities might be set by other countries at the international level where individual MSs would not be in a strong position to influence decisions.	Increased networking between European/ International experts	0	0	**0**
		Enhanced dialogue about social aspects of security and resilience	0	0	**0**
		Higher citizens' trust in Information Society services and systems	-	1	**0**
		Better safeguarding of fundamental rights through enhancing protection of CII	0	0	**0**
		Environmental			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	0	0	**0**

Option 2: Implementation of measures within a non-binding framework

Objective	Action	Impact	Magnitude	Likelihood	Total
Specific objective 1: Bridging gaps on national policies for the security and resilience of CII (Option 2)					
Operational objective 1.1 Enhancing the cooperation on policy areas that constitute the common ground of national approaches to security and resilience of CII	**Action 1.1.1** The Commission would work with Member States in identifying transferable examples of public policy practices and commonalities. Such activity would benefit from stock-taking and analysis of existing commonalities, building upon existing studies and analysis.	**Economic**			
		Less costs for companies operating in more MSs due to reduced differences in obligations concerning security and resilience	++	2	++++
		Economies of scale in implementing security obligations for companies operating in more MSs	++	2	++++
		Enhanced know-how	++	2	++++
		More investments triggered by common policy objectives and standards for security and resilience at EU level	++	2	++++
		More users and use due to increased confidence	+	2	++
		Lower operational risks for business due to higher level of security and resilience of CII	+++	2	++++++
		Social			
		Increased networking between European / International experts	+++	2	++++++
Operational objective 1.2 Information sharing and exchange of good policy practices	**Action 1.2.1** The Commission would establish a European Forum for Member States to share information and good policy practice on security and resilience for CII. The activity would benefit from the result of the work and operational activities conducted by other organisations (e.g. ENISA).	Enhanced dialogue about social aspects of security and resilience	++	2	++++
		Equal levels of protection of EU citizens' personal data and privacy due to enhanced security of CII	++	2	++++
		Higher citizens' trust in Information Society services and systems	+	1	+
		Better safeguarding of fundamental rights through enhancing protection of CII	++	2	++++
		Environmental			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	+	1	+
		Better use of energy for ICT due to better rationalisation of the security and resilience measures	++	2	++++
		Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	++	2	++++

Objective	Action	Impact	Magnitude	Likelihood	Total
Specific objective 2: Enhancing the European governance for the security and resilience of CII (Option 2)					
Operational objective 2.1 Knowledge sharing to deepen the understanding of challenges for the security and resilience of CII	**Action 2.1.1** The Commission would establish a European Public-Private Partnership, to support cooperation and information sharing on European and global challenges for the security and resilience of CII. The primary focus would be on the European dimension of the challenges for security resilience of CII, both from a strategic (e.g. good practices for public policy) and tactical/operational (e.g. industrial deployment) perspective. To this end, the PPP would build upon and complement both existing national initiatives as well as the operational work conducted by ENISA. Topics to be discussed in the context of such partnership may include: - processes for vulnerability disclosure - practices for threat identification - methodologies for risk assessment - common terminology and procedures for the collection and dissemination of information on economic impacts of security incidents - workable frameworks and practices to support the exchange of sensitive information.	**Economic**			
		Increased availability of information on challenges and risks for security and resilience	+++	2	++++++
		Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual MS	++	2	++++
		Efficient management due to better governance mechanisms	++	2	++++
		Enhanced know-how	++	2	++++
		More investments triggered by common policy objectives and standards for security and resilience at EU level	++	2	++++
		Lower risks of catastrophic failures/accidents in Europe	+	1	+
		Lower operational risks for business due to higher level of security and resilience of CII	+++	2	++++++
		Social			
		Increased networking between European/ International experts	++	2	++++
	Action 2.1.2 The Commission would analyse the methodological and legal challenges related to the collection and dissemination of information on the economic impacts of security incidents. To this end, a study on the economic implications of the security and resilience of CII should be launched in 2009, under the eCommunications budget line. The results of these activities would feed into the work of the European partnership planned in Action 2.1.1.	Enhanced dialogue about social aspects of security and resilience	++	2	++++
		Better response to cyber attacks and cyber disruptions	++	2	++++
		Better safeguarding of fundamental rights through enhancing protection of CII	+	2	++
		Environmental			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	+	1	+
Operational objective 2.2 Identification and dissemination of good practices	**Action 2.2.1** In the context of FP7 or other programmes, the Commission would launch, where appropriate, calls for research projects aimed at identifying prospective challenges (and possible solutions) to enhance the security and resilience of CII.	Better use of energy for ICT due to better rationalisation of the security and resilience measures	+	2	++
		Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	++	2	++++

Objective	Action	Impact	Magnitude	Likelihood	Total
Specific objective 3: Strengthening Europe's operational incident response capability (Option 2)					
Operational objective 3.1 The identification and agreement on a minimum level of capabilities and services for well-functioning National/Governmental CERTs and the Establishment of well-functioning National/Governmental CERTs	**Action 3.1.1** The Commission would work with Member States on defining the appropriate baseline of capabilities, services and operational functions for National/Governmental CERTs. The definition and a wide adoption of such a baseline would reinforce the national response capability and ensure that national capabilities could cooperate at the European and international levels.	**Economic**			
		Increased availability of information on challenges and risks for security and resilience	+++	2	++++++
		Enhanced operational know-how	+++	2	++++++
	Action 3.1.2 The Commission would encourage and support (inter alia by promoting good practices and guidelines) Member States to establish well-functioning National/Governmental CERTs with the aim to integrate their function/operation more in a public policy dimension. In addition to their operational function, National/Governmental CERTs could play the role of catalysers of stakeholder interests and capabilities for public policy activities, including those related to establishing national information and alert sharing systems to reach out to citizens and SMEs, which constitute the national building blocks for EISAS. The activity would benefit from the work conducted by ENISA in the context of its CERT-related activities.	Less costs of cyber attacks due to better preparedness and faster response	+++	2	++++++
		More users and use due to increased confidence	+	1	+
		More competitive SMEs due to better knowledge, more information and more support to tackle security risks	++	1	++
Operational objective 3.2 Development of Operational Contingency Plans and Performance of Exercises	**Action 3.2.1** The Commission would stimulate and support Member States in developing national operational contingency plans for CII. To this end, the Commission would organise meetings / conferences to exchange experience, lessons learnt and 'good practices'. The establishment of national contingency plans would be instrumental for stronger cooperation and coordination towards European-wide operational contingency plan. This activity would also be supported via the forum planned in Action 1.2.1, where common strategic objectives could be discussed. ENISA could be asked to support these exchanges by providing its expertise on the operational dimension of this challenge.	Lower risks of catastrophic failures/accidents in Europe	+++	2	++++++
		Lower operational risks for business due to higher level of security and resilience of CII	++	2	++++
		Social			
	Action 3.2.2 The Commission would facilitate the Member States to design and perform pan-European exercises to test contingency plans, which would involve all relevant	Increased networking between European/ International experts	+++	2	++++++

Objective	Action	Impact	Magnitude	Likelihood	Total
	stakeholders. This would be organised via the financial support in WP2009 of DG JLS Programme on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks". Member States and stakeholders would, where appropriate, build upon the ENISA "CSIRT Exercise book" and the exercises planned by ENISA in 2009.	Equal levels of protection of EU citizens' personal data and privacy due to enhanced security of CII	++	2	++++
Operational objective 3.3 reinforcement of operational co-operation and dialogue between National/Governmental CERTs	**Action 3.3.1** The Commission would stimulate Member States to further develop and reinforce the pan-European cooperation among well-functioning National/Governmental CERTs. To this end, existing organisations such as the European Governmental CERTs Group (EGC) could be leveraged. In addition, the Commission would ask ENISA to continue and augment its activities aimed at reinforcing the capabilities of CERTs in Europe as well as encouraging operational cooperation and dialogue amongst National/Governmental CERTs. The cooperation would also be reinforced by the step-wise development of a European Information Sharing and Alert Systems whose building blocks would be national information and alert sharing systems, for which National/Governmental CERTs are a key resource. These activities would also build upon the results of the study planned in Action 3.3.2, as well as on the results of the 2 prototype implementations of EISAS being funded under WP2008 of the Programme on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks" (DG JLS).	Better reaching out citizens	+++	2	++++++
		Better response to cyber attacks and cyber disruptions	+++	2	++++++
		Better quality of services to citizens and SME's of better quality due to lower level of disruptions	++	1	++
		Higher citizens' trust in Information Society services and systems	+	1	+
		Environmental			
	Action 3.3.2 The Commission would launch a study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet. It is expected that the results of this study would also contribute to the reinforcement of operational co-operation and dialogue between National/Governmental CERTs.	Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	+	1	+
		Better use of energy for ICT due to better rationalisation of the security and resilience measures	+	2	++
Operational objective 3.4 clarification of legal obstacles to the exchange of information on incidents and providing collaborative platforms for ensuring the confidentiality of information	**Action 3.4.1** The Commission would take the lead in promoting the discussion of workable frameworks to support the exchange of sensitive information. Such action could leverage the Public-Private Partnership planned in Action 1.2.1.	Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	++	2	++++

Objective	Action	Impact	Magnitude	Likelihood	Total
Specific objective 4: Enhancing Internet security and resilience (Option 2)					
Operational objective 4.1 Defining EU priorities for Internet long term stability and resilience	**Action 4.1.1** The Commission would involve all relevant stakeholders in defining a set of European public policy priorities for Internet stability and resilience. To this end, the Commission would organise meetings and/or participate in relevant fora.	**Economic**			
		Increased availability of information on challenges and risks for security and resilience	++	2	++++
	Action 4.1.2 The Commission would strengthen its interaction with key European Internet Governance actors (i.e. CENTR and RIPE) in order to devise a common set of EU priorities for Internet stability and resilience.	Efficient management due to better governance mechanisms	++	2	++++
		Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual MS	++	2	++++
	Action 4.1.3 The Commission would launch a study on DNS resilience in order to identify the main challenges to ensure the security and resilience of the global Domain Name System, one of the key critical infrastructures of the Internet. The study would be funded under the 2008 Programme on "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks" (DG JLS). The results of this activity will be instrumental for the definition of EU priorities for Internet long term stability and resilience.	Enhanced know-how	++	2	++++
		More users and use due to increased confidence	++	2	++++
		Less costs of cyber attacks due to better preparedness and faster response	++	2	++++
		Lower risks of catastrophic failures/accidents in Europe	++	2	++++
		Social			
	Action 4.1.4 In the context of FP7 or other programmes the Commission would closely monitor the projects focused on Internet stability and resilience and use the results of such projects to define the EU priorities in the area under consideration.	Increased networking between European/ International experts	++	2	++++
		Enhanced dialogue about social aspects of security and resilience	++	2	++++
Operational objective 4.2 Launching a European-led international initiative with aim to create a set of principles for Internet security and resilience	**Action 4.2.1** The Commission would define a first proposal of a set of principles for Internet security and resilience. To this end, due account would be taken of existing initiatives and of the work of other relevant organisations (such as the OECD, ICANN, the Internet Governance Forum, ITU, etc).	Higher citizens' trust in Information Society services and systems	+	1	+
		Better safeguarding of fundamental rights through enhancing protection of CII	++	2	++++
	Action 4.2.2 The Commission would propose and take the lead in defining a roadmap for an international initiative aimed at creating a set of principles for Internet security and resilience. To this end, strategic cooperation with third countries will be developed, in particular with countries like USA, Canada and Japan, as a vehicle to build global consensus.	**Environmental**			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	+	1	+

Option 3: Establishment of a binding framework

Objective	Action	Impact	Magnitude	Likelihood	Total
Specific objective 1: Bridging gaps on national policies for the security and resilience of CII (Option 3)					
Operational objective 1.1 Enhancing the cooperation on policy areas that constitute the common ground of national approaches.	The Commission would propose binding measures to define a baseline that would harmonise national policies. Such measures may focus on additional security and resilience of CII (for instance, those that relate to obligations for mutual assistance, priority calls, emergency services, continuity of services for vital functions, etc.) that would be outside the framework of the market legislation already proposed (i.e. the review of the e-communication Regulatory Package).	**Economic**			
		Less costs for companies operating in more MSs due to reduced differences in obligations concerning security and resilience	++	1	++
		Economies of scale in implementing security obligations for companies operating in more MSs	++	1	++
		Enhanced know-how	+	1	+
		More investments triggered by common policy objectives and standards for security and resilience at EU level	+	1	+
		More users and use due to increased confidence	++	2	++++
		Lower operational risks for business due to higher level of security and resilience of CII	+	1	+
		Social			
Operational objective 1.2 Information sharing and exchange of good policy practices		Increased networking between European / International experts	+	1	+
		Enhanced dialogue about social aspects of security and resilience	+	1	+
		Equal levels of protection of EU citizens' personal data and privacy due to enhanced security of CII	++	2	++++
		Higher citizens' trust in Information Society services and systems	+	1	+
		Better safeguarding of fundamental rights through enhancing protection of CII	++	2	++++
		Environmental			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	+	1	+
		Better use of energy for ICT due to better rationalisation of the security and resilience measures	+	1	+
		Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	+	1	+

Objective	Action	Impact	Magnitude	Likelihood	Total
Specific objective 2: Enhancing the European governance for the security and resilience of CII (Option 3)					
Operational objective 2.1 Knowledge sharing to deepen the understanding of challenges for the security and resilience of CII	The Commission would propose binding measures to define the role and responsibility of public and private stakeholders in security and resilience of CII for possible situations and scenarios.	**Economic**			
		Increased availability of information on challenges and risks for security and resilience	+	1	+
		Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual MS	+	1	+
		Efficient management due to better governance mechanisms	+	2	++
		Enhanced know-how	+	1	+
		More investments triggered by common policy objectives and standards for security and resilience at EU level	+	1	+
		Lower risks of catastrophic failures/accidents in Europe	+	1	+
		Lower operational risks for business due to higher level of security and resilience of CII	++	1	++
Operational objective 2.2 Identification and dissemination of good practices		**Social**			
		Increased networking between European/ International experts	+	1	+
		Enhanced dialogue about social aspects of security and resilience	++	1	++
		Better response to cyber attacks and cyber disruptions	++	1	++
		Better safeguarding of fundamental rights through enhancing protection of CII	+	2	++
		Environmental			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	+	1	+
		Better use of energy for ICT due to better rationalisation of the security and resilience measures	+	1	+
		Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	+	1	+

Objective	Action	Impact	Magnitude	Likelihood	Total
Specific objective 3: Strengthening Europe's operational incident response capability (Option 3)					
Operational objective 3.1 The identification and agreement on a minimum level of capabilities and services for well-functioning National/Governmental CERTs and the Establishment of well-functioning National/Governmental CERTs	The Commission would propose binding measures to improve operational preparedness. The first element would be a minimal set of standard for harmonised level functions and services for National/Governmental CERTs, with a view to make them contribute to a centrally organised European incident response capability. The second element would be a framework for national contingency planning with a view to develop EU wide contingency plans.	**Economic**			
		Increased availability of information on challenges and risks for security and resilience	+	1	+
		Enhanced operational know-how	++	2	++++
		Less costs of cyber attacks due to better preparedness and faster response	++	1	++
		More users and use due to increased confidence	+	2	++
Operational objective 3.2 Development of Operational Contingency Plans and Performance of Exercises		More competitive SMEs due to better knowledge, more information and more support to tackle security risks	+	1	+
		Lower risks of catastrophic failures/accidents in Europe	++	1	++
		Lower operational risks for business due to higher level of security and resilience of CII	++	1	++
Operational objective 3.3 reinforcement of operational co-operation and dialogue between National/Governmental CERTs		**Social**			
		Increased networking between European/ International experts	+	1	+
		Equal levels of protection of EU citizens' personal data and privacy due to enhanced security of CII	++	2	++++
		Better reaching out citizens	+	1	+
		Better response to cyber attacks and cyber disruptions	++	2	++++
		Better quality of services to citizens and SME's of better quality due to lower level of disruptions	++	1	++
Operational objective 3.4 clarification of legal obstacles to the exchange of information on incidents and providing collaborative platforms for ensuring the confidentiality of information		Higher citizens' trust in Information Society services and systems	+	1	+
		Environmental			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	+	1	+
		Better use of energy for ICT due to better rationalisation of the security and resilience measures	+	1	+
		Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	+	1	+

Objective	Action	Impact	Magnitude	Likelihood	Total
Specific objective 4: Enhancing Internet security and resilience (Option 3)					
Operational objective 4.1 Defining EU priorities for Internet long term security and resilience	There is no possible short-term binding measure that can be taken for achieving operational objectives 4.1 and 4.2 – see sec. 5.5.	**Economic**			
		Increased availability of information on challenges and risks for security and resilience	-	1	-
		Efficient management due to better governance mechanisms	--	2	----
		Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual MS	--	2	----
		Enhanced know-how	0	0	**0**
		More users and use due to increased confidence	-	1	-
		Less costs of cyber attacks due to better preparedness and faster response	--	2	----
		Lower risks of catastrophic failures/accidents in Europe	--	2	----
		Social			
Operational objective 4.2 Launching a European-led international initiative with aim to create a set of principles for Internet security and resilience		Increased networking between European/ International experts	0	0	**0**
		Enhanced dialogue about social aspects of security and resilience	0	0	**0**
		Higher citizens' trust in Information Society services and systems	-	1	**-**
		Better safeguarding of fundamental rights through enhancing protection of CII	0	0	**0**
		Environmental			
		Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	0	0	**0**

ANNEX 4: COMPARISON OF THE IMPACTS

Specific objective 1: Bridging gaps on national policies for the security and resilience of CII						
Impacts	**Option 1**		**Option 2**		**Option 3**	
	Magnitude	Likelihood	Magnitude	Likelihood	Magnitude	Likelihood
Economic						
Less costs for companies operating in more MSs due to reduced differences in obligations concerning security and resilience	---	1	++	2	++	1
Economies of scale in implementing security obligations for companies operating in more MSs	---	2	++	2	++	1
Enhanced know-how	0	0	++	2	+	1
More investments triggered by common policy objectives and standards for security and resilience at EU level	--	2	++	2	+	1
More users and use due to increased confidence	-	1	+	2	++	2
Lower operational risks for business due to higher level of security and resilience of CII	--	2	+++	2	+	1
Social						
Increased networking between European/International experts	0	0	+++	2	+	1
Enhanced dialogue about social aspects of security and resilience	0	0	++	2	+	1
Equal levels of protection of EU citizens' personal data and privacy due to enhanced security of CII	--	2	++	2	++	2
Higher citizens' trust in Information Society services and systems	-	1	+	1	+	1
Better safeguarding of fundamental rights through enhancing protection of CII	0	0	++	2	++	2
Environmental						
Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	0	0	+	1	+	1
Better use of energy for ICT due to better rationalisation of the security and resilience measures	-	1	++	2	+	1
Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	-	1	++	2	+	1
Specific objective 2: Enhancing the European governance for the security and resilience of CII						
Impacts	**Option 1**		**Option 2**		**Option 3**	
	Magnitude	Likelihood	Magnitude	Likelihood	Magnitude	Likelihood
Economic						
Increased availability of information on challenges and risks for security and resilience	-	1	+++	2	+	1
Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual MS	--	2	++	2	+	1
Efficient management due to better governance mechanisms	--	2	++	2	+	2
Enhanced know-how	0	0	++	2	+	1
More investments triggered by common policy objectives and standards for security and resilience at EU level	-	2	++	2	+	1
Lower risks of catastrophic failures/accidents in Europe	--	2	+	1	+	1
Lower operational risks for business due to higher level of security and resilience of CII	--	2	+++	2	++	1

Social						
Increased networking between European/International experts	-	2	++	2	+	1
Enhanced dialogue about social aspects of security and resilience	0	0	++	2	++	1
Better response to cyber attacks and cyber disruptions	--	2	++	2	++	1
Better safeguarding of fundamental rights through enhancing protection of CII	0	0	+	2	+	2
Environmental						
Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	0	0	+	1	+	1
Better use of energy for ICT due to better rationalisation of the security and resilience measures	--	1	+	2	+	1
Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	--	1	++	2	+	1
Specific objective 3: Strengthening Europe's operational incident response capability						
Impacts	**Option 1**		**Option 2**		**Option 3**	
	Magnitude	Likelihood	Magnitude	Likelihood	Magnitude	Likelihood
Economic						
Increased availability of information on challenges and risks for security and resilience	--	1	+++	2	+	1
Enhanced operational know-how	--	1	+++	2	++	2
Less costs of cyber attacks due to better preparedness and faster response	--	2	+++	2	++	1
More users and use due to increased confidence	-	1	+	1	+	2
More competitive SMEs due to better knowledge, more information and more support to tackle security risks	--	2	++	1	+	1
Lower risks of catastrophic failures/accidents in Europe	--	2	+++	2	++	1
Lower operational risks for business due to higher level of security and resilience of CII	--	2	++	2	++	1
Social						
Increased networking between European/International experts	0	0	+++	2	+	1
Equal levels of protection of EU citizens' personal data and privacy due to enhanced security of CII	-	1	++	2	++	2
Better reaching out citizens	-	1	+++	2	+	1
Better response to cyber attacks and cyber disruptions	--	2	+++	2	++	2
Better quality of services to citizens and SME's of better quality due to lower level of disruptions	--	1	++	1	++	1
Higher citizens' trust in Information Society services and systems	-	1	+	1	+	1
Environmental						
Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	0	0	+	1	+	1
Better use of energy for ICT due to better rationalisation of the security and resilience measures	-	1	+	2	+	1
Lower damage to the environment because of propagation of disruptions to CII to environmentally critical infrastructures	-	1	++	2	+	1
Specific objective 4: Enhancing Internet security and resilience						

Impacts	Option 1		Option 2		Option 3	
	Magnitude	Likelihood	Magnitude	Likelihood	Magnitude	Likelihood
Economic						
Increased availability of information on challenges and risks for security and resilience	-	1	++	2	-	1
Efficient management due to better governance mechanisms	--	2	++	2	--	2
Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual MS	--	2	++	2	--	2
Enhanced know-how	0	0	++	2	0	0
More users and use due to increased confidence	-	1	++	2	-	1
Less costs of cyber attacks due to better preparedness and faster response	--	2	++	2	--	2
Lower risks of catastrophic failures/accidents in Europe	--	2	++	2	--	2
Social						
Increased networking between European/ International experts	0	0	++	2	0	0
Enhanced dialogue about social aspects of security and resilience	0	0	++	2	0	0
Higher citizens' trust in Information Society services and systems	-	1	+	1	-	1
Better safeguarding of fundamental rights through enhancing protection of CII	0	0	++	2	0	0
Environmental						
Reduced impact of CO2-emmissons from less travel due to higher reliance on the use of CII	0	0	+	1	0	0

ANNEX 5: EUROPEAN COMMISSION POLICY INITIATIVES RELATED TO NETWORK AND INFORMAION SECURITY

1. INTRODUCTION

The purpose of this note is to briefly present the main policy initiatives of the European Commission that are related to network and information security and relevant to the forthcoming policy on critical information infrastructures protection (CIIP).

2. THE STRATEGY FOR A SECURE INFORMATION SOCIETY

In May 2006, the Commission adopted a **Communication** on a Strategy for a Secure Information Society[1]

This Communication identified several key challenges facing Network and Information Security (NIS) to include:

- Attacks on information systems increasingly motivated by profit rather than by the desire to create disruption for its own sake.
- The increasing deployment of new forms of communication platforms and information systems such as mobile devices and mobile-based network services which provide new opportunities for malicious attacks.
- The 'advent' of 'ambient intelligence' in which intelligent devices supported by computing and network technology will become ubiquitous and therefore create additional security and privacy-related risks.
- The impact of breaches in NIS can transcend the economic dimension and may lead to user discouragement and lower take-up of ICT; availability, reliability and security are a prerequisite for guaranteeing user's rights on-line.
- Both businesses and citizens in Europe still underestimate the risks.
- There is an increased dependency of other critical infrastructures (like transport, energy etc) on the integrity of their respective information systems which are more and more interconnected with other networks.
- An insufficient awareness by the stakeholders of their responsibility in the overall security chain.
- A fragmentation of the European NIS market.

To tackle these challenges, the Commission proposed a multi-stakeholder approach based on dialogue, partnership and empowerment as the mechanisms to engage stakeholders in enhancing security of the Information Society. The actions include:

- To address the evolution of spam and threats such as spyware and other forms of malware.
- To improve cooperation between law enforcement authorities and addressing new forms of criminal activity that exploit the Internet and undermine the operation of critical infrastructures.
- To develop a sector-specific approach for ICT to examine the relevant economic, business and societal drivers with a view to enhancing the security and the resilience of networks and information systems in the framework of the European Programme for Critical Infrastructure Protection (EPCIP).[2]

---

1 COM (2006) 251, 31.5.2006.

2 COM (2006) 786, 12.12.2006.

- To consider elements to improve NIS in the review of the regulatory framework for electronic communications,[3] such as technical and organisational measures to be taken by service providers, provisions dealing with the notification of security breaches, and specific remedies and penalties regarding breaches of obligations.
- To encourage the private sector to deliver solutions, services and security products to end users so that European industry be both a demanding user of security products and services as well as a competitive supplier of NIS products and services.
- To promote actions to build trust and consumer confidence.
- To achieve a holistic approach that recognises the respective roles of the various stakeholders.
- To promote global cooperation on NIS.
- To allocate appropriate financial resources to research on NIS and dependability technologies under the 7th EU Framework Programme for Research & Development (FP7).

The Communication identified several areas for involvement of ENISA in contributing to the strategy, including:

- Examining the feasibility of creating a European multilingual information sharing and alert system.
- Developing a trusted partnership with Member States and stakeholders to develop an appropriate data collection framework, including the procedures and mechanisms to collect and analyse EU-wide data on security incidents and consumer confidence.
- Playing an active role in a dialogue with SMEs and citizens, and in consolidating and exchanging best practices.
- Assisting the Member States in raising awareness on the virtues, benefits and rewards of adopting effective security technologies, practices and behaviour.

In March 2007, the **Council** adopted a **Resolution** in which it welcomed the Communication of the European Commission.[4]

The key challenges identified were in line with those of the strategy of the Commission. Notably, the impacts with regards to:

- The development of new technologies rapidly moving us towards a ubiquitous information society and networks.
- The increasingly central role that electronic network and information systems play in the society and in particular in the overall operation of Critical infrastructures. As a consequence, this central role stresses how the availability and integrity of electronic network and information systems become indispensable to administrations', businesses, citizens' safety and quality of life, as well as to overall functioning of societies.

The Council resolution also welcomed the intention of the Commission to "*encourage the Member States to examine, via a multi-stakeholder dialogue, the economic, business and societal drivers with the aim of developing an ICT sector-specific policy to enhance the security and resilience of network and information systems, as a potential contribution to the planned European Programme on Critical Infrastructure Protection.*"

Lastly, it stressed that the establishment of ENISA has been "*a major step forward in the EU's efforts to respond to the challenges relating to network and information security*", and

[3] The review started in 2006 and is expected to complete by end of 2008.

[4] Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe, OJ C 68/01 of 24.3.2007.

welcomed the intention of the Commission to strengthen "*the involvement of ENISA in supporting the Strategy for a Secure Information Society in Europe.*"

3. OTHER COMMISSION INITIATIVES AND PROPOSALS RELATED TO NIS

3.1. Communication on fighting spam, spyware and malicious software

In November 2006, the European Commission put forward a Communication on fighting spam, spyware and malicious software.[5]

The challenges identified were the evolution of spyware and malicious codes as well as spam becoming increasingly fraudulent and criminal in nature.

The actions laid out reinforced the solutions proposed in the Strategy. At EU level, actions put forward were as follows:

- To continue efforts in raising awareness and fostering cooperation between stakeholders.
- To continue to develop agreements with third countries including on the fight against spam, spyware and malware.
- To introduce new legislative proposals at the beginning of 2007 that strengthen the rules in the area of privacy and security in the communications sector and present a policy on cyber crime.
- Involve ENISA expertise in security matters.
- Support research and development within the FP7 program.

3.2. Communication on data protection by privacy enhancing technologies

In May 2007, the European Commission issued a Communication on promoting data protection by Privacy Enhancing Technologies[6] (PETs) in order to achieve a high level of protection of privacy and personal data in Europe.

The Commission proposed to involve a vast array of actors including its own services, national authorities, industry, consumers: to support the development of PETs, to support the use of available PETs by data controllers and to encourage consumers to use PETs (particularly through awareness raising activities).

3.3. Communication on the fight against cyber crime

In May 2007, the European Commission issued a Communication on the fight against cyber crime.[7]

The main challenges identified concerned the fact that the number of cyber crimes was growing and that criminal activities had become increasingly sophisticated and internationalised. At the same time, the number of European prosecutions on the basis of cross-border law enforcement cooperation did not increase.

---

5 COM (2006) 688, 15.11.2006
6 COM (2007) 228, 2.05.2007
7 COM(2007)267, 22.5.2007

In order to tackle the increasingly significant number of threats affecting critical infrastructures, society, business and citizens, the proposed actions included:

- Further development of specific instruments in the fight against cyber crime to:
  - strengthen operational law enforcement cooperation and EU-level training efforts.
  - strengthen the dialogue with industry.
  - continue efforts with a view to harmonise Member States' legislation.
  - consider legislation against identity theft.
  - develop statistical data (indicators for measuring the extent of cyber crime).
- Actions of a general nature concerning illegal content and the fight against traditional crime perpetrated via electronic networks.

3.4. The Safer Internet Programme

Over the years, the European Union has set legal standards to fight illegal and harmful content and, more in general, address on line risks for children. Since 1999 the Commission has funded activities at national and European levels to promote the safer use of the Internet and other online technologies. On 27 February 2008, the Commission adopted a proposal for a new Safer Internet programme[8] that builds upon the achievements of the Safer Internet *plus* Programme. Four main actions are proposed:

- Reducing illegal content and tackling harmful conduct online;
- Promoting a safer online environment;
- Ensuring public awareness and
- Establishing a knowledge base for addressing existing and emerging uses, risks and consequences.

International cooperation will be encouraged as an integral part of each of these actions.

3.5. International cooperation

Network and information security cover far-reaching and global issues that require coordinated international efforts. Previous initiatives established that there is a need for closer cooperation at global level to improve security standards, exchange threat information, and promote a common approach to network and information security issues.

Responses to a public consultation on an EU Strategy for International Cooperation on ICT[9] highlighted several priority areas for cooperation to include:

- Harmonisation of legal regimes and consistent regulatory framework related to network and information security;
- Fighting spam, fishing, malware and distributed denial-of-service (DDoS) attacks as well as protecting critical information infrastructures and improving the security and robustness of the information society;
- Promoting emergency response exercises; fostering enhanced cross-border collaboration on key information infrastructure functions; making recommendations of general character for Critical Information Infrastructure Protection (CIIP) measures based on best practices; and undertaking significant efforts to ensure the integrity of key components of this infrastructure.
- Enhancing the exchange of information on security threats and incidents, promoting the dissemination of best practices and increase the level of education and awareness raising;

---

[8] Proposal for a Decision of the European Parliament and of the Council establishing a multi-annual Community programme on protecting children using the Internet and other communication technologies, COM (2008) 106, 27. 2. 2008.

[9] See http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=356.

- The promotion and funding of international research in NIS and supporting high R&D investment in this field.

Critical Information Infrastructure Protection has an important trans-national dimension, in particular with regard to Internet. The World Summit on the Information Society (WSIS) has emphasised that security and stability of Internet have to be maintained. Therefore this concern represents one of the key strands also in the post WSIS discussions. There is a major challenge addressed to the key players across Europe, but also internationally, to be engaged in order to organise a coordinated EU, or international action.

The European Union will continue to play its part in fostering cooperation with the global community. In particular, the EU follows the developments in the context of the Internet Governance Forum where security related issues are discussed in a multi-stakeholder environment. The European Commission also participates in the discussions on the security of the information society in international organisations such as the OECD.

3.6. The Reform of the telecoms regulatory framework[10]

In November 2007, the European Commission issued a package of Proposals to reform the regulatory framework for electronic communications[11]. The reform proposals address several privacy and security issues, including:

- The proposed new Articles 13a and 13b within the Framework directive foresee provisions to strengthen operators' obligations to safeguard the security of their networks or services, including necessary steps to ensure the integrity of their networks so as to ensure the continuity of supply of services provided over those networks.[12]
- The proposed Article 13a also includes provisions for mandatory notification of the national regulatory authorities (NRAs) of any breach of security or integrity that had a significant impact on the operation of networks or services.
- Proposed provisions for Article 4 of Directive 2002/58/EC on privacy and electronic communications include requirements of mandatory notification of the subscriber in case of a breach of security related to personal data.[13]

3.7. European Programme on Critical Infrastructure Protection (EPCIP)

The **European Council of June 2004** asked for the preparation of an **overall strategy to protect critical infrastructure**. In response, the **Commission adopted on 20 October 2004** a Communication "Critical Infrastructure Protection in the Fight Against Terrorism" putting forward clear suggestions on what would **enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructures**.

The **Council** conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" adopted in **December 2004 endorsed** the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP).

---

10 This section will have to be updated after the first reading vote in the EP on 23 September.

11 See http://ec.europa.eu/information_society/policy/ecomm/library/proposals/index_en.htm.

12 Proposal for a Directive of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services, COM(2007) 697 of 13.11.2007.

13 Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, COM(2007) 698 of 13.11.2007.

The **Commission** adopted in **December 2006** a Communication on a Programme for Critical Infrastructures Protection (EPCIP) and a proposal for a Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. In June 2008, the Council of the European Union reached a political agreement on a directive on the identification and designation of the European Critical Infrastructures and the assessment of the need to improve their protection[14] that constitutes one of the main elements of EPCIP. The formal adoption of this directive is expected by the end of the year. In the final version of the directive, the ICT sector is referred to as the next a priority sector after energy and transport.

4. THE ENISA REGULATION AND THE EVALUATION OF THE AGENCY

The legal basis for the ENISA Regulation is Article 95 of the Treaty establishing the European Community. This means that the activities of ENISA contribute to regulatory measures[15] which have as their object the establishment and functioning of the internal market. Following an action brought by the United Kingdom against the legal basis, the European Court of Justice confirmed that the Regulation was rightly based on Article 95.[16]

ENISA has carried out actions in several areas of network and information security activities, among which feature prominently those on:

- Collecting appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them.
- Building a trusted partnership with Member States and stakeholders to develop an appropriate data collection framework on security incidents and levels of consumer confidence.
- Advising and assisting the European Commission and the Member States on information security and in their dialogue with industry.
- Facilitating cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues.
- Examining the feasibility of a European information sharing and alert system to facilitate effective responses to existing and emerging threats to electronic networks.
- Awareness-raising and co-operation between different players in the information security field, notably by developing public/private partnerships with industry.

To assess the options for the review of the Regulation before its expiry in March 2009, the Commission launched an evaluation that was conducted by an external panel of experts.[17] The key findings of that expert report confirmed the validity of the policy resulting in the creation of ENISA and its original goals, and in particular its contribution to achieving a truly internal market in electronic communications. Further to the expert report, the Management Board of ENISA issued recommendations regarding the eventual changes to the Regulation[18] where it supports the extension of the mandate of the Agency without materially changing its scope.

---

14 See http://register.consilium.europa.eu/pdf/en/08/st09/st09403.en08.pdf

15 "Measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States."

16 Judgment of 2 May 2006 in Case C-217/04.

17 Evaluation of the European Network and Information Security Agency", Final Report by the Experts Panel, IDC EMEA, 8.1.2007 (Available at: http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en .htm).

18 Available at: http://enisa.europa.eu/pages/01_05.htm.

4.1. The public consultation

In June 2007, the Commission issued a Communication on the evaluation of ENISA[19] which provides an appraisal of the evaluation conducted by the external group of experts and launched a public consultation on the way forward in summer 2007. The responses to the public consultation included the following observations.

- The majority of respondents considered that the threat landscape has evolved since ENISA was established: challenges changed in nature and increased in complexity. Attacks became more targeted and more difficult to detect. Hackers became motivated by financial means or political motivation rather than 'show-off'. Increased use of networks, emerging technologies, the need to improve the level of security in software, and vulnerability of important IT infrastructures pose further challenges. In addition, the globalisation of threats and global interdependencies magnified a need for enhanced international cooperation and coordination. Most respondents agreed that an Agency was still the right instrument to deal with these challenges.
- A broad majority of respondents agreed that extended objectives, be it operational or regulatory, should not be foreseen for ENISA. A few respondents suggested some areas in which ENISA could develop operational activities.
- A majority of respondents considered that the future role and tasks of ENISA should be clarified in order to establish the ideal size of ENISA's staff and budget. However, many of the respondents identified the need for the ratio between administrative and operational staff to be revised so as to enhance the impact of ENISA on network and information security.

5. TOWARDS A STRENGTHENED NETWORK AND INFORMATION SECURITY POLICY IN EUROPE – PUBLIC CONSULTATION

In September 2008, the European Parliament and the Council, when they adopted the extension of the mandate of ENISA, called for *"further discussion on the future of ENISA and on the general direction of the European efforts towards an increased network and information security."*[20] In June 2008, the Council had asked the Commission to contribute to this discussion.[21]

On 2nd September, in her intervention during the Plenary Session of European Parliament, Commissioner Reading called on "the European Parliament and the Council to open, early in 2009, an intense debate on Europe's approach to network security and on how to deal with cyber-attacks, and to include the future of ENISA in those reflections." She also stated that in order to facilitate such a debate "the Commission services will, in the second half of 2008, develop a questionnaire to be submitted to public online consultation on the possible objectives of a modernised NIS policy at EU level, and on the means to achieve those

---

19 COM(2007) 285.

20 See Recital 5, which called for "*further discussion on the future of ENISA. The discussion will reflect the results of the ENISA evaluation process, the Management Board recommendations and the ongoing review of the Regulatory Framework for electronic communications networks and services. It will also allow further reflection on the general direction of the European efforts towards an increased network and information security. The extension of the duration of the Agency is without prejudice to the outcome of this discussion.").*

21 Draft minutes of the 2877th meeting of the Council of the European Union (Transport, Telecommunications and Energy), held in Luxembourg on 12 and 13 June 2008 (10641/08), which specifies: "The Council agreed on a General Approach as set out in 10338/08 and formally asked the Commission to contribute to a future discussion on ENISA and on the general direction of the European efforts towards an increased network and information security.

objectives. This will, of course, be done in consultation with ENISA and its management board."

On 7th November, the Commission launched an online public consultation[22] on the possible objectives of a strengthened NIS policy at EU level, and on the means to achieve those objectives. The objective and scope of the public consultation takes into account that the Commission's forthcoming policy initiative on Critical Information Infrastructure Protection (CIIP) would be an important contribution to enhance NIS. The consultation will be closed on 9th January 2009. The responses to this public consultation will be published and analysed by the Commission services in a separate **internal** report.

[22] See http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464

ANNEX 6: EU RESEARCH ACTIVITIES IN THE AREA OF NETWORK AND INFORMATION SECURITY

Under the FP7 ICT Theme the Commission funds 110 M€ over 2007-2008 for research in the area of ***Secure and trustworthy network and service infrastructures***,
In the context of the COM on CIIP, we emphasise the following sub-areas:

1. Research in the area of protection of critical information infrastructures, with a total budget of 20 million Euros.

The focus of this research will be on protecting the Internet and other ICT networks and systems with their interconnections to other Critical Infrastructures (for energy distribution, transport, finance etc.).
More precisely, following an FP7 call for R&D proposals that that was launched late 2007 jointly with the Security programme **nine ICT projects have been selected under the ICT programme.** They are all expected to be operational by this autumn. The main research areas that these projects cover include:

- Understanding and managing the interactions and complexity of interdependent critical infrastructures; adding resilience to the telecommunications networks, aimed at emergency situations;

- Building secure and resilient networked process control (SCADA) systems and secure and fault-tolerant wireless sensor and actuator networks operating in critical infrastructures; safeguarding critical financial infrastructures or protecting the functioning of underwater wireless network infrastructures operating in off-shore platforms and energy plants

2. Research for protecting the Internet and other ICT infrastructures against emerging threats and vulnerabilities

It addresses assessment and management of security levels of networks, content and services; early detection, monitoring and countering of attacks and intrusions; and novel threat prevention mechanisms.
About 10 M€ funding is spent on this work. Examples of research carried out in these projects are:

- Early identification and modelling of emerging cyber-threats through collection and analysis of security-related raw data (R&D project WOMBAT, http://www.wombat-project.eu);

- Tools for monitoring the traffic of networks for detecting frauds and attacks while preserving the privacy of communications and protecting users' data (R&D project PRISM, http://www.fp7-prism.eu/).

- Fostering collaboration and partnership between academia and industry against cyber-threats (viruses, botnets and spyware), spam and phishing (Coordination Action FORWARD, http://www.ict-forward.org).

- Increasing software security by bridging the gap between security experts and software practitioners and by providing the software developers with the means to effectively prevent occurrences of known vulnerabilities when building software (R&D project SHIELDS, http://shields-project.eu/).

3. Research in identity management schemes

A third topic relevant in this context is identity management schemes that improve the secure interaction of users with digital systems and services, while respecting the users' privacy and personal data. Such research work can substantially contribute to fighting against cyber-criminality, as it helps establishing the right level of accountability and responsible use in the Internet, while protecting users' rights and freedom. **Two FP7 ICT projects** carry out research in this direction, for about **7.5 million EUR EU funding**:

- Building a cross-layer identity management framework for network infrastructures by extended identity functions and network federations, addressing usability and privacy concerns (R&D project SWIFT, http://www.ist-swift.org)

- A platform providing privacy-enhanced identity and trust management for complex community-supporting services that are built on Next Generation Networks (R&D project PICOS, http://www.picos-project.eu).

ANNEX 7: THE ESTONIAN CASE

WHAT HAPPENED?

At the end of April, news reports and official statements by Estonian governmental representatives reported a significant cyber-attack on multiple targets in Estonia, including banks and government offices. These attacks appear to have continued for several weeks resulting in appeals by the Estonian government for EU and NATO partners to treat them as an act of terrorism against the Estonian state.

NATO subsequently sent experts to Tallinn, prior to Estonian Defence Minister Jaak Aaviksoo asking for NATO to set out a clear policy for cyber defence at a meeting in Brussels on May 14.

- What was the nature of the attack?

The main information available at the moment is from press reports and statements from Estonian government officials quoted in the press. Not surprisingly, given the nature of such attacks, there is little "hard" information in the public domain.

That said, it is clear that a large number of governmental and non-governmental organisations in Estonia have been subjected to a prolonged attack on their information systems which has resulted in widespread disruption in their abilities to provide services on-line. Available information strongly suggests that the main cause of disruption was a **"Distributed Denial of Service" (DDoS)** attack**.**

DDoS attacks work by infecting the machines of innocent users with malware that gives control to the party who wrote the malware. If the initial distribution of the malware is effective in infecting sufficient machines, the result is a global network of compromised machines known as a "bot-net" (short for a robot network) that can then be used to attack another system. The target system will then find itself subject to significant levels of incoming traffic way above anything it is designed to cope with under normal operating circumstances. At this point, the target system can no longer cope, being unable to differentiate between "legitimate" incoming traffic and that generated by zombies. At this point the only solution is often to disconnect the system from the public Internet until the attacks stop, denying service to legitimate users and zombies alike.

- How can you tell who has launched such an attack?

Unfortunately, due to the nature of such attacks, **they can be difficult but not impossible to track back to the originator**. Traffic data can be used to identify the zombies generating the traffic, but these are normally the property of innocent third parties who are unaware that their machines have been used in criminal activities. Examination of the source of their infection may just lead to another zombie, so examination of traffic data is not normally helpful.

That said, analysis of the malware itself can help determine who the instigator of the attack was (and who can of course be on a different continent from the zombie machines). The propagators of such attacks can however, be very technically skilled and structure a bot-net and its associated virus in such a way as to deliberately suggest the origin of the attack is somewhere else. **This is always likely to create an element of doubt in any investigation.**

- Was the Estonian attack just another DDoS?

DDos attacks are familiar to those fighting cyber-crime and responsible for IT security, although the Estonian situation is notable for several reasons:

- The scale of the attack (a very large number of targets)
- The duration of the attack (several weeks)
- The nature of the target (effectively the "state" rather than a single organisation)
- The fact that a specific country was targeted

Indeed, the scale of the attack suggests that this may have been the single largest DDoS ever launched, possibly using multiple botnets.

What is clear is that the attacks on Estonia **need careful analysis** to try and identify the origin of the attacks and in order to learn whatever lessons we can to prepare for, and minimise the impact of, future attacks. Moreover, there are likely to be elements of such analysis that **need to be treated confidently** for obvious reasons.

WHAT IS THE ROLE OF THE EU?

- ENISA

The creation of a **European Agency for Network and Information Security (ENISA)** was an important step in creating a comprehensive and effective EU approach to such matters based on a Commission proposal from 2003. It is true that Member States acting in the Council did not want ENISA to have any operational responsibilities but its mandate does provide for the first time for a specific institution to focus at European level on these priority issues.

In the wider context, it is also important to note the ongoing work on Critical Infrastructure Protection (CIP) which covers all key infrastructure (energy, transport, communications etc) and related activities under the EU CIP programme. There are operational limits to the activities that can be coordinated at EU level due to the sovereignty sensitivities of Member States but there is a clear added value in enabling cooperation between Member States at EU on such important issues.

WHAT IS THE ROLE OF THE COMMISSION IN SUCH MATTERS?

It is inevitable that some aspects of the incidents in Estonia are **matters of Estonian national sovereignty** where it will be for the Estonian government to decide what action to take and what support they would like to receive from international partners and institutions such as the EU.

That said, the Commission has been pushing the security & stability of IT systems and infrastructure to the top of the political agenda for years. Last year, for example, the Commission proposed a comprehensive policy approach to information security issues in it's **communication** "A strategy for a Secure Information Society – Dialogue, partnership and empowerment". In this communication, the Commission requested ENISA to investigate the feasibility of an European Information Sharing and Alert Systems (EISAS), which could build on existing national systems and be of benefit for the EU citizens. Such a system would help share and pool together information and knowledge from existing EU capabilities to help facing crises like that of the attack on Estonian networks.

National CERTs and CSIRTs (Computer Security Incidents Response Teams) also cooperate together across countries via initiatives and organisations like FIRST, TERENA, the European Government CERT Group, etc. However, the cooperation at the EU level is far from being optimal in terms of geographical and country coverage. In view of this, initiatives

have been launched to strengthen the cooperation between CERTs/CSIRTs, including a specific action by the Commission (namely DG INFSO) in the eEurope 1998 Action Plan. Nowadays, facilitating the cooperation between European CERTs/CSIRTs is one of the activities of the European network and Information Security Agency (ENISA). ENISA is a first pillar Agency but is neither a CERTs/CSIRTs nor has operational tasks similar to those of CERTs/CSIRTs.

Discussions on security-related issues are, and will continue to be, a regular feature of the multiple dialogues the Commission has with the Member states and other key stakeholders in other areas such as research and cybercrime.

THE INTERNATIONAL DIMENSION

It is important to recognise that **other institutions** such as NATO have a particular and important role to play in addressing issues such as those we have seen in Estonia.

NATO has a particularly strong role given that Estonia is a member of the NATO CERT system. (CERTs are Computer Emergency Response Teams set up to offer early-warning alerts when security incidents occur and for launching appropriate procedures to counteract such threats).

In addition, in the **World Summit on Information Society** (2003-2005), the Commission was in the forefront of participants arguing that security & stability needs to be the key **over-riding priority for governments** as IT systems such as the Internet become so central to our economic and social life. Specifically, since the World Summit, the Commission and the EU in general has been explicitly pushing for the launching of international discussions on "enhanced cooperation" to discuss relevant issues, among the most important of which is security & stability.

COULD THE EU DO MORE DO MORE?

One additional step that could be taken is to seek increased cooperation at the level of public administrations (involving both the Commission and the Member States) in relation to the European Government CERT Group. This would involve:

- an invitation to all Member States to create CERTs (not all have them at the moment) and to then participate actively in the Government Group.
- A parallel initiative could be to propose the creation of an EU Institutions CERT to support and participate in the same group.

The EU could consider creating an operational functionality at EU level, either by:

- extending the mandate of ENISA or
- in the context of an agency for electronic communications or
- by creating an agency for critical infrastructure.

It is also worth considering the possibility of extending the current cooperative warning networks that exist in Member states to deal with public safety, food etc (Warning and Information Networks - CWINs) to encompass threats to information systems.

ANNEX 8: EXAMPLES OF PUBLIC-PRIVATE PARTNERSHIPS

In the US a major contribution in this area was provided by the establishment of the Information and Analysis Centres (ISACs). Created in response to a government directive (US Presidential Decision Directive 63) ISACs are private sector organisations responsible for collecting, distributing, analysing, and sharing sensitive information concerning threats, vulnerabilities, alerts and best practices. Due to their structure and mandate, ISACs have somewhat helped in overcoming private companies' resistance to sharing information with competitors. A confidentiality mechanism is a necessary element of any reporting process, and it must be operated such as to engender the trust required to allow the system to work. ISACs gather operators active in the same commercial sector, e.g. financial services, information technology, energy, transportation etc. Today there are fourteen critical infrastructures with an active ISAC, eleven of which have joined together under the umbrella of the ISAC Council. ISACs were mostly conceived with a distinct technical focus rather then political or legal, and this helped make them a source of knowledge extremely valued by public sector. The possible negative aspect of this system is a degree of reluctance to make that information available outside the ISAC.

Another model is represented by the UK ***Warning Advice and Reporting Points*** (WARP), which are community-based services whose members receive and share up-to-date advice on information security threats, incidents and solutions. Initially launched by NISCC and currently part of the CPNI's Information Sharing Strategy, the WARP model is conceived to address the needs of those constituencies which could not support an own CERT capability. WARPs provide three types of services: (i) filtered warnings ('customized' on recipient needs); (ii) advice brokering (a secure environment to discuss 'good practices'); (iii) trusted sharing of sensitive information. However, unlike CERTs, the WARPs are unable to provide technical response services. WARPs are developed within homogeneous small groups where trusted relationships already exist. Membership in WARPs is voluntary.

ANNEX 9: EXAMPLES OF PUBLIC-PRIVATE PARTNERSHIPS IN MEMBER STATES

Public Private Partnerships (PPP) at national level play an important role in almost all MS that responded to the questionnaire prepared by the European Commission (see section 1.2 of the IA report). The involvement of the private sector to foster preparedness is considered essential given the fact that many ICT critical infrastructures are owned by private companies due to the liberalization process. Some contributors provided examples of PPP at national level:

- (EE) pointed out that its national cyber defence is greatly based on PPP which have developed into an efficient network and have created a favourable environment among all parties involved. PPP at international level is considered desirable but difficult to implement because it mostly depends on the good will of private sector actors to cooperate. In order to solve this problem at national level, these partnerships have been launched in certain specific areas where a considerable number of stakeholders are interested (e.g. financial institutions as well as major ISPs have been interested and very active in participating in joint activities).
- (HU) the Ministry in charge of Informatics and Communication contracted a Foundation to operate the national CERT. In addition, a project was launched to provide the general public with a website containing information on IT security issues such as spam, viruses, and other threats and on the possibilities to protect privacy in an easy understandable manner; The Theodore Puskás Foundation was established in 1992. It was co-founded by the government of Hungary and several distinguished institutions and businesses. It operates as a non-profit, public benefit organization. Its main objective is the dissemination of advanced technologies in Hungary. The foundation's activities include scientific research, consultations, and instruction in the field of information technologies. In 2004, the Ministry of Informatics and Communication contracted the foundation to operate the national Computer Emergency Response Team (CERTHungary), in consideration of its good reputation of the foundation and its research experiences in the field of information technology
- (SE) A National Crisis Management Co-ordination group has been set up (NTGC). The group works on a voluntary basis where members from major telecommunications providers and the NRA work regularly on a bilateral level on how to establish robust electronic communication. The group 1) is based on experience from national cross-sector exercises, Heavy storms and other lessons learned. 2) Is a voluntary co-operative forum with members from major telecommunications providers as well as the Swedish Urban Network Association, the Armed Forces and the National Post- and Telecom Agency, PTS. 3) Chair: the National Post- and Telecom Agency, PTS. 4) Has the aim to support the restoration of the national infrastructure for electronic communications during critical disturbances in our society, such as terrorism, extreme weather… 5) The individuals representing each member are of great importance for their own network operation. The group will meet ´virtually´ and need secure communications
- (PL) ARAKIS-GOV is an example of private public partnership. The system has been developed by CERT Poland team which operates within NASK (Scientific and Academic Computer Networks which is financed from public funds and was implemented in cooperation with a governmental agency. Currently the system is operated jointly by CERT Poland and the governmental computer emergency response team CERT GOV PL.

- (UK) The UK Government relies on partnerships with industry to understand and enhance the level of protection of critical infrastructure. Information exchanges between the public and the private sector are a good example of this in practice. A specific example is provided by UK's Centre for the Protection of National Infrastructure (CPNI). CPNI runs an information exchange platform located in the buildings of the Minister of Defence. This location is considered as neutral from the point of view of regulation. This platform has the merit to gather around the same table large vendors who are not used to speak one to the others being fierce competitors (eg CISCO and Juniper). The vendors' representatives who participate to the information exchange are neither from sales or marketing departments nor from government affairs units. They are technical experts. Groups of discussion are set-up according to the professional profile of the company. There is an information exchange group dedicated for ICT vendors and an other one for telecom operators and so on (vertical organisation). The traffic light protocol is used to exchange information. A non disclosure agreement is signed by the participant. This platform is considered as a useful forum for trust.
- (DK) BERIT is a forum formed in DK to promote dialogue between infrastructure owners, users and public bodies. Three meetings have been organised so far. In order to create trust, participants were asked to demonstrate security clearance. The objective of the forum is to promote dialogue between infrastructure owners and users and as such to contribute to an effective and efficient level of preparedness and continuity, focusing on the need of society. The users are asked to share their own preparedness experience and knowledge of technical trends. The owners of infrastructures are demanded to share information on preparedness and key vulnerabilities. The regulator has to share information on planned actions. Some 20 entities participate to the forum from the sectors of Defence (including first respondents, civil protection), National Health, Transport, Broadcasting, Operators – fixed and mobile ISP, the Regulator. The national IT and Telecom Agency provides the secretariat to the group.
- (FI) National Emergency Supply Council (NESC, previously National Board of Economic Defense) under the auspices of the Ministry of Employment and the Economy, supports and assists NESA activities. NESC also plans and coordinates economic preparations for implementation in case of exceptional circumstances in Finland. NESC is a network of committees consisting of the leading experts from both the public administration and the business world. Its tasks are to analyze threats against the country’s security of supply, to plan measures to control these threats, and to promote readiness planning in individual industrial sites. NESC’s areas of responsibility include the Information Society, transport logistics, food supply, energy supply, healthcare services, financial services, and defense-related and other critical industrial sectors. NESC members include representatives of ministries, government agencies, the private business sector, and various industrial organizations.
- (FR) The Strategic Advisory Board on Information Technologies (CSTI)27 was created in July 2000 at a meeting of the government committee on the Information Society. It is chaired by the French prime minister. The CSTI is composed of business and industry executives and leading representatives of the research and development community. It is responsible for recommendations to government concerning CIIP topics and the French contribution to the 6th European Framework Research and Development Program.
- (DE) the development of the CIP implementation plan, followed by a set of ongoing activities to actually implement measures. The CIP implementation plan was prepared in close cooperation between representatives of critical infrastructure operators and service

providers as well as experts from the federal administration. The plan aims at implementing measures that make it possible to bring the goals of operators in the private industry in line with the higher-level (safeguarding) interests of the community. The plan addresses the need for measures that meet security requirements extending beyond the security and business continuity responsibilities within the enterprises, as well as the aim of encouraging industries to scrutinize their own security and risk management approaches.

- (IT) The Association of Italian Experts for Critical Infrastructures is a not-for-profit organization that aims "to support an interdisciplinary and inter-sectoral culture for the development of strategies, methodologies, and technologies supporting the correct management of Critical Infrastructure during periods of crisis, in case of exceptional events, and during terrorist attacks or natural disasters." The AIIC comprises public as well as private members. In order to raise awareness of information security and critical infrastructure protection, the association publishes periodical newsletters on national and international developments in the field of CIIP and provides information on strategies and policies as well as on recent scientific findings on its website.
- (NL) The Platform Electronic Commerce in the Netherlands (ECP.NL) has been tasked by the Ministry of Economic Affairs with setting up a public-private partnership program to implement the action guidelines of the KWINT Memorandum. The objective of the KWINT program focused on the following aspects: continuity of the internet infrastructure in the Netherlands, viruses, denial-of-service attacks, hacking, transparency of internet services, integrity and confidentiality of information, and misuse by personnel. The Strategic Board for CIP (Strategisch Overleg Vitale Infrastructuur, SOVI) was established in September 2006 as a dedicated public-private partnership for critical infrastructure protection. All critical sectors are represented in the strategic board, which meets two or three times a year. In 2007, the SOVI initiated a study on the electric power dependency of the various critical sectors and their resilience and ability to cope with longer duration power outages. It investigated issues such as secondary dependencies (e.g., dependency of various sectors on diesel oil for back-up generators) and the way in which these are prioritized amongst the critical sectors. It also studied the question of which related arrangements already exist or have yet to be made.

ANNEX 10: GLOSSARY

- **Botnet** –a group of computers, often very large, that malicious hackers have brought under their control. While most owners are oblivious to the infection, the networks of tens of thousands of computers are used to launch spam e-mail campaigns, denial-of-service attacks or online fraud schemes.

- **BSA** – Business Software Alliance.

- **ccTLD** – country code top-level domain.

- **CERT** – Computer Emergency Response Team: an organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems and to limiting damage and ensure continuity of critical services in spite of successful attacks, accidents, or failures.

- **CSIA** - Cyber Security Industry Alliance.

- **CSIRT** – Computer Security Incident Response Team. (A CSIRT is a service organisation that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporation, governmental, or educational organisation; a region or country; a research network; or a paid client.)

- **Distributed Denial of Service (DDoS)** – an attempt to make a computer resource unavailable to its intended users.

- **Domain Name Registry –** an organisation that manages the registration of Domain names within the top-level domains for which it is responsible, controls the policies of domain name allocation, and technically operates its top-level domain. It is potentially distinct from a domain name registrar.

- **DNS** - Domain Name System

- **ECTA** – European Competitive Telecommunications Association

- **ENISA** – The European Network and Information Security Agency was created following the adoption of Regulation (EC) No 460/2004 of the European Parliament and of the Council on 10 March 2004 "for the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market". www.enisa.europa.eu

- **EPCIP** – European Programme for Critical Infrastructure Protection.

- **ESA** – The European Software Association is an industry body set up by some of best know companies in Europe whose business is to develop and market software.

These businesses are usually known as ISVs or Independent Software Vendors (in other countries, referred to as Software Developers, Software Editors or similar phrase). http://www.europeansoftware.org

- **ETNO** – European Telecommunications Network Operators' Association. ETNO was established in May 1992 and has become the principal policy group for European electronic communications network operators. ETNO's primary purpose is to establish a constructive dialogue between its member companies and decision-makers and other actors involved in the development of the European Information Society to the benefit of users. www.etno.be

- **EuroISPA** – the pan-European association of the Internet services providers associations of the countries of the European Union; the world's largest association of ISPs. www.euroispa.org

- **EuroIX** – European Internet Exchange Association

- **Internet** – global system of interconnected computer networks that interchange data by packet switching using the standardized Internet Protocol Suite (TCP/IP).

- **Internet protocol (IP)** – a protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite (TCP/IP).

- **ISAC** – Information Sharing and Analysis Center

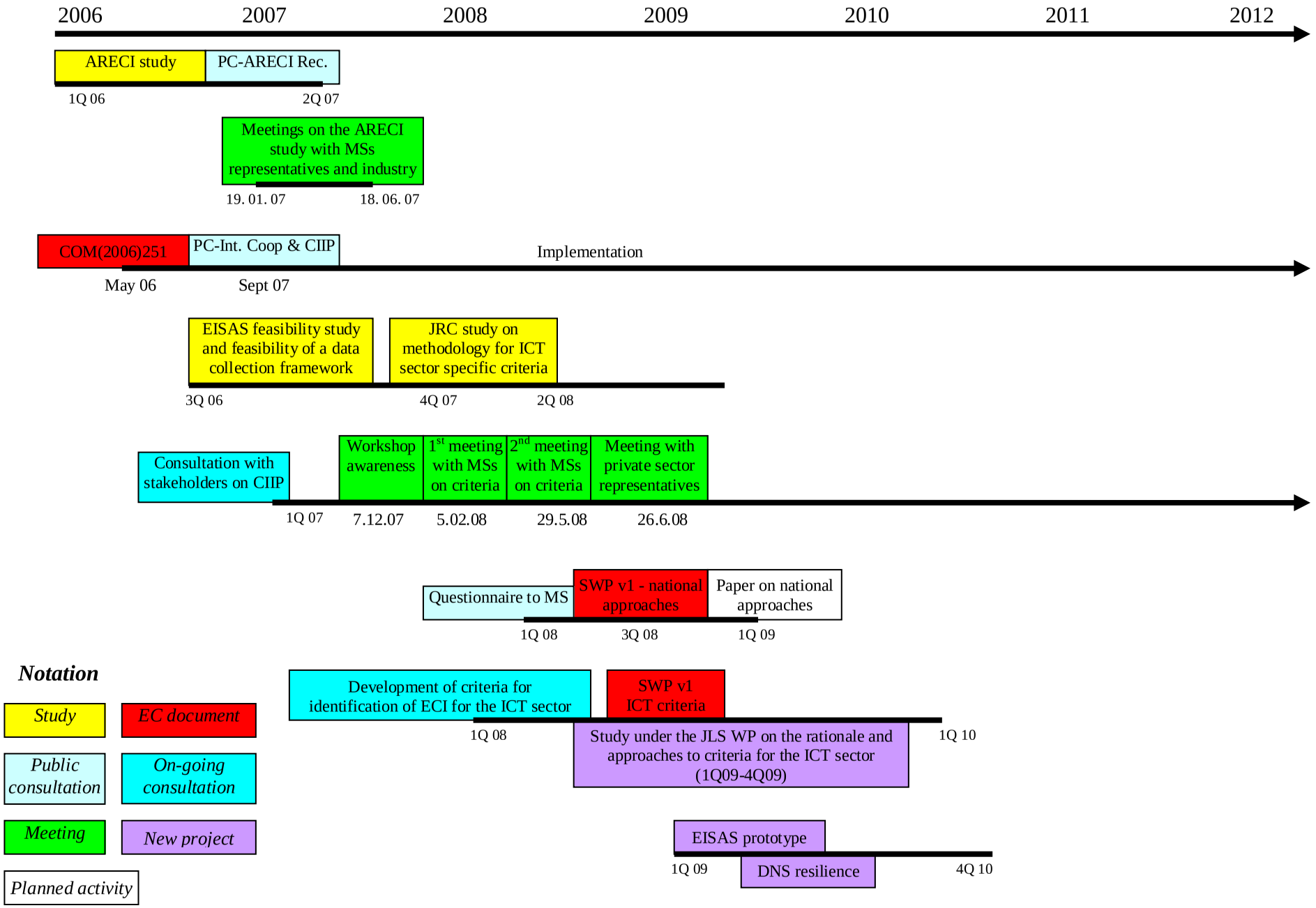
- **Malware** – a commonly used abbreviation for for malicious software and "is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, whether it's a virus, spyware, et al" – see http://www.microsoft.com/technet/security/alerts/info/malware.mspx.

- **Resilience** – the ability of a system to recover from adversity, either back to its original state or an adjusted state based on new requirements. Building resilience requires a long-term effort involving reengineering fundamental processes, both technical and social.

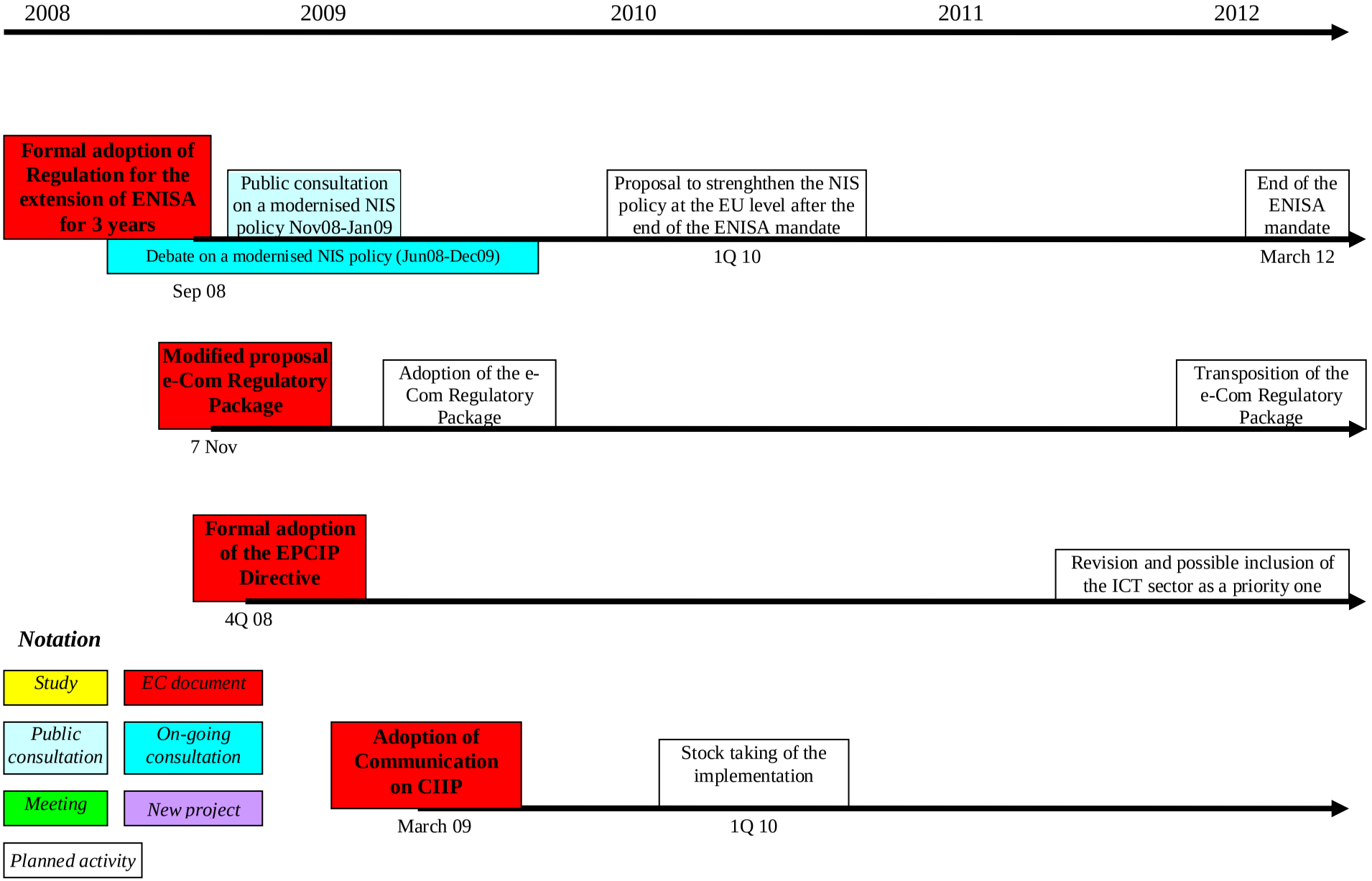
- **RIPE NCC** – Réseaux IP Européens (French for "European IP Networks). The RIPE NCC is an independent, not-for-profit membership organisation that supports the infrastructure of the Internet through technical co-ordination in its service region. The most prominent activity of the RIPE NCC is to act as the Regional Internet Registry (RIR) providing global Internet resources and related services (IPv4, IPv6 and AS Number resources). The membership consists mainly of Internet Service Providers (ISPs), telecommunication organisations and large corporations located in Europe, the Middle East and parts of Central Asia

ANNEX 11: TIMELINE OF COMMISSION ACTIVITIES RELATED TO CIIP

PART 1: PREPARATORY ACTIVITIES



PART 2: IMPLEMENTATION ACTIVITIES



ANNEX 12: THE ARECI STUDY

European Commission
Information Society and Media Directorate-General

AVAILABILITY AND ROBUSTNESS OF ELECTRONIC COMMUNICATIONS INFRASTRUCTURES

"The ARECI Study"

Final Report

March 2007

This page is intentionally left blank

Prepared by:

Bell Labs and Professional Services

This page is intentionally left blank

Preface

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

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

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

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

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

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

This page is intentionally left blank

Table of Contents

Table of Figures

Table of Tables

This page is intentionally left blank

1. EXECUTIVE SUMMARY

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

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

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

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

Guiding Principles of Study

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

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

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

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

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

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

Methodology of Study

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

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

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

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

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

100 Key Findings of Study

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

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

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

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

Maturity Level 1

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

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

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

Maturity Level 3

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

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

Impact: To the extent that critical calls are attempted on public networks, the probability of call completion is not consistent with the urgency of such calls if

they are not provided preferential treatment on public networks. The use of public networks provides the critical stakeholders with ubiquitous access, extra capacity, and resiliency.

Maturity Level 4

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

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

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

10 Recommendations of Study

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

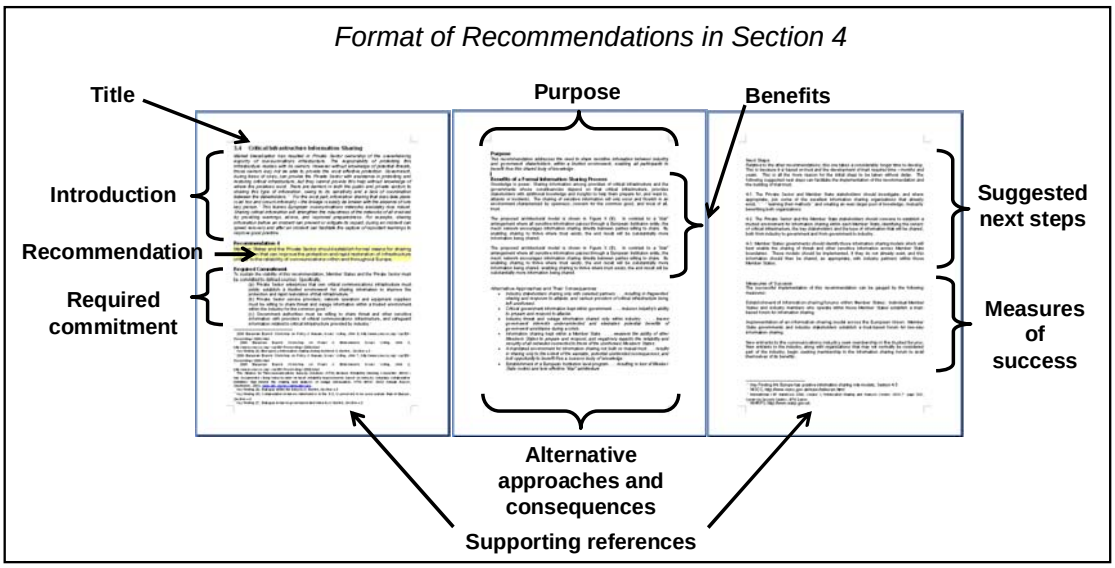


Figure 1: Presentation of Recommendations in Section 4

1. Emergency Preparedness *improve the speed of response*

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

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

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

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

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

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

integrated into the architecture of future networks so that the public networks can be used to extend emergency communications capabilities.

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

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

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

3. Formal Mutual Aid Agreements *enhance network resilience*

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

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

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

Required Commitment

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

4. Critical Infrastructure Information Sharing *informing each other*

Issue

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

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

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

Purpose

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

Recommendation

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

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

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

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

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

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

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

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

Issue

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

Purpose

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

Recommendation

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

Required Commitment

The required commitment to implement this Recommendation is high because of differences between the everyday visibility of concrete competitive pricing pressure, which the consumer enjoys, and the less tangible reality of the factors described above. European Institutions and Member States must face their vital dependence on Information and Communications Technology (ICT) and articulate a vision that properly stresses the importance of trusted hardware, software and networks. In addition, European Institutions and Member States should encourage, by policy and

economic incentive, research that supports the development and implementation of supply-chain processes and safeguards that provide assurances for technology trustworthiness. Further, European Institutions and Member States should provide incentives for Private Sector investment by awarding government communications services contracts to those service providers most aligned with these principles to improve security and reduce vulnerabilities. Finally, the Private Sector needs to continuously pursue technology improvements in the quality and control of their supply chains across the product lifecycle (e.g., design, development, deployment, support) to increase the security assurance of information and communications systems.

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

Issue

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

Purpose

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

Recommendation

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

Required Commitment

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

8. Interoperability Testing *a level playing field*

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

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

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

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

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

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

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

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

Required Commitment

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

10. Discretionary European Expert Best Practices *harnessing expertise*

Issue

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

Purpose

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

Recommendation

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

Required Commitment

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

Summary

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

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

Europe's future communications networks promise to usher in a new world of business and lifestyle-enhancing capabilities – many of which have not yet even been imagined. Relatively recent advances of ICT in the areas of affordable pricing, mobility, geo-locating, video imaging and search engines, while breathtaking, are

likely only the beginning of an ever-accelerating pace of the same for the foreseeable future. While the urgency is pressing, the long term benefits of reliable communications networks are incomparable. The people of Europe stand to greatly benefit from the anticipated economic efficiency, citizen connectivity, functional flexibility, and speed. This Study strongly urges the European Commission, Member States and Private Sector stakeholders to chart and embark on a new course of policy and practice that forcefully advocates highly available and highly robust communications infrastructure.

This page is intentionally left blank

2. INTRODUCTION

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

2.1. Mission

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

The following statement represents the purpose of this Study:

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

2.2 Scope

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

2.2.1 Terms of Reference

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

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

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

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

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

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

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

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

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

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

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

[2] A more formal definition: The degree to which a system, subsystem, or equipment is operable and in a committable state at the start of a mission, when the mission is called for at an unknown (i.e. a random) time.
Glossary contains a more complete definition, including mathematical formula.
[3] wordnet.princeton.edu/perl/webwn.
[4] www.onesixsigma.com/tools_resources/glossary/glossary_r.php
[5] Institute of Electrical and Electronics Engineers. *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.* New York, NY: 1990.
[6] www.bitpipe.com/tlist/Telecommunications-Infrastructure.html.
[7] K. R. Rauscher, R. E. Krock, J. P. Runyon, "Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security" Bell Labs Technical Journal, 11(3), 73-78 (2006) ©Lucent Technologies Inc. Published by Wiley Periodicals Inc. Published online at Wiley Interscience (www.interscience.wiley.com).

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

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

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

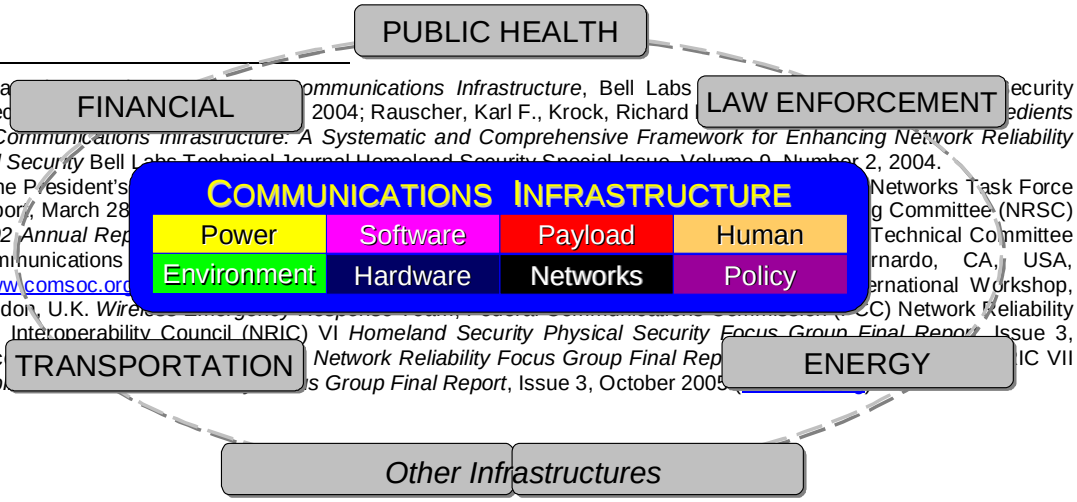
- **Networks:** Networks include the various topological configurations of nodes, synchronisation, redundancy, and physical and logical diversity.

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

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

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

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



[8] Ra… *…ommunications Infrastructure*, Bell Labs … ecurity Spec… 2004; Rauscher, Karl F., Krock, Richard … *…edients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security* Bell L… Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004.

[9] The President's … Networks Task Force Repor… March 28… …g Committee (NRSC) *2002 Annual Rep…* …Technical Committee Communications … …rnardo, CA, USA, (www.comsoc.org… …ernational Workshop, London, U.K. *Wirel…* …(CC) Network Reliability and Interoperability Council (NRIC) VI *Homeland Security Physical Security Focus Group Final Report*, Issue 3, Dec… *Network Reliability Focus Group Final Rep…* …IC VII *Publ…* …*s Group Final Report*, Issue 3, October 2005…

Figure 2: Eight Ingredient Framework of Communications Infrastructure

2.2.2 Network and Technology

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

Network Access Types

This Study considered the following network access types:

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

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

Network Technologies

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

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

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

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

Subscriber Service Types

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

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

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

2.3 Principles of Approach

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

- *Keep the interests of the citizens* of Europe in the forefront
- *Be forward-looking* in technology considerations, factoring in trends
- Uphold *European focus*, yet maintain global awareness
- *Be inclusive* in receiving all European insights offered
- *Ensure rich representation* of industry, academic and government perspectives, with care to include both embedded as well as new entrants

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

- *Utilise world-class proficiency* in both the technical subject matter and broader policy areas to ensure the output would be both realistic and achievable
- *Fulfil the formal requirements* for the Study's execution

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

2.4 Participants

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

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

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

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

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

Table 1: Organisations that contributed to the Study

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

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

SYMANTEC
TDC
Telecom Italia
Telefonica Deutschland
Telefonica Moviles
Telefonica O2 Cz
Telefonica Spain
TeliaSonera
The Open University
T-Mobile
TP S.A
T-REGS bvba
T-Systems
TVCABO
UKERNA
University of Bristol
US Mission to the EU
Verisign
Verizon Business
Vodafone Italy

A.

B.

C.

D.

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

2.4.1 Private Sector

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

Industry Roles

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

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

Sector Stakeholders

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

---

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

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

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

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

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

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

2.4.2 Academia

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

2.4.3 Government

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

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

2.4.4 Other Aspects of Representation

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

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

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

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

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

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

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

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

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

2.5 Methodology

The ARECI Study was conducted over a period of approximately one year. The methodology used a custom-designed approach for the special needs of the mission. The special needs of the mission included the following aspects. First and foremost, the work is very important as the availability and robustness of public networks is crucial for many reasons, the most crucial being that it can be a factor in saving lives. Secondly, because the heart of this Study deals with critical infrastructure, it is of immediate interest for Member States both from a sovereignty and socio-economic perspective. Thirdly, the Private Sector is simultaneously managing increased competition and wide sweeping technological changes. The final aspect is the global

security environment that includes both increased concern of terrorist attack and the possibility of a remote cyber attack from another part of the world. The approach designed for this Study addresses these four concerns through various means.

2.5.1 The Eight Ingredient Framework

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

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

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

Intrinsic Vulnerability Analysis

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

As part of this Study, subject matter experts were polled as to which of the intrinsic vulnerabilities (complete list provided in Annex B) caused them the greatest concern regarding Europe's future networks. Their concerns were instrumental in developing many of the Key Findings (Section 3) and Recommendations (Section 4).

[17] Annex B.

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

Table 2: Intrinsic Vulnerabilities of Greatest Concern

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

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

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

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

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

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

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

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

Outdated ASPR	**45%**	**2, 7, 10**
Unimplemented ASPR (complete or partial)	**45%**	**7, 8, 10**

2.5.2 Collaboration

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

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

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

2.5.3 Confirmation of Best Practices

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

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

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

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

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

of these workshops was a major basis for the Key Findings and Recommendations made in this Study.

European Experts Workshops

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

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

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

Effectiveness

Best Practice Selection Criteria

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

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

POWER BEST PRACTICES

- Network Operators, Service Providers, Equipment Suppliers and Property Managers should develop documentation for the restoration of power for areas of critical infrastructure including such things as contact information,

[20] These best practices were previously developed by global communications companies and have been shown to be beneficial to European network operators and equipment suppliers.
[21] Best Practice EU06-5204 can be referred to as BP 5204. The EU06 is used to track when the Best Practice was last modified.
[22] Best Practices for six of the eight ingredients have been defined. Two of the ingredients (Environment, Human) received insufficient votes to be statistically significant, and therefore no European Best Practices have as yet been identified for these two ingredients.

escalation procedures, restoration steps and alternate means of communication. This documentation should be maintained both on-site and at centralised control centres. EU06-5231

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

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

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

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

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

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

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

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

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

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

- Network Operators, Service Providers and Property Managers should consider placing generator sets and fuel supplies for critical sites within a

secured area to prevent unauthorised access, reduce the likelihood of damage and/or theft, and to provide protection from explosions and weather. EU06-5212

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

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

HARDWARE BEST PRACTICES

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

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

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

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

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

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

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

SOFTWARE BEST PRACTICES

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

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

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

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

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

NETWORK BEST PRACTICES

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

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

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

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

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

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

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

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

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

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

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

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

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

- Schedule System Backups: Network Operators and Service Providers should establish policies and procedures that outline how critical network element databases will be backed up onto a storage medium (e.g., tapes, optical diskettes) on a scheduled basis. EU06-0603
- Network Operators and Service Providers should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network, before it is placed into service. EU06-0612

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

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

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

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

PAYLOAD BEST PRACTCIES

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

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

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

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

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

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

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

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

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

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

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

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

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

POLICY BEST PRACTICES

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

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

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

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

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

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

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

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

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

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

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

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

- Sharing Information with Law Enforcement: Network Operators, Service Providers and Equipment Suppliers should establish a process for releasing information to members of the law enforcement and intelligence communities

and identify a single Point of Contact (POC) for coordination/referral activities. EU06-8065

Cost and Risk

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

Cost to Implement

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

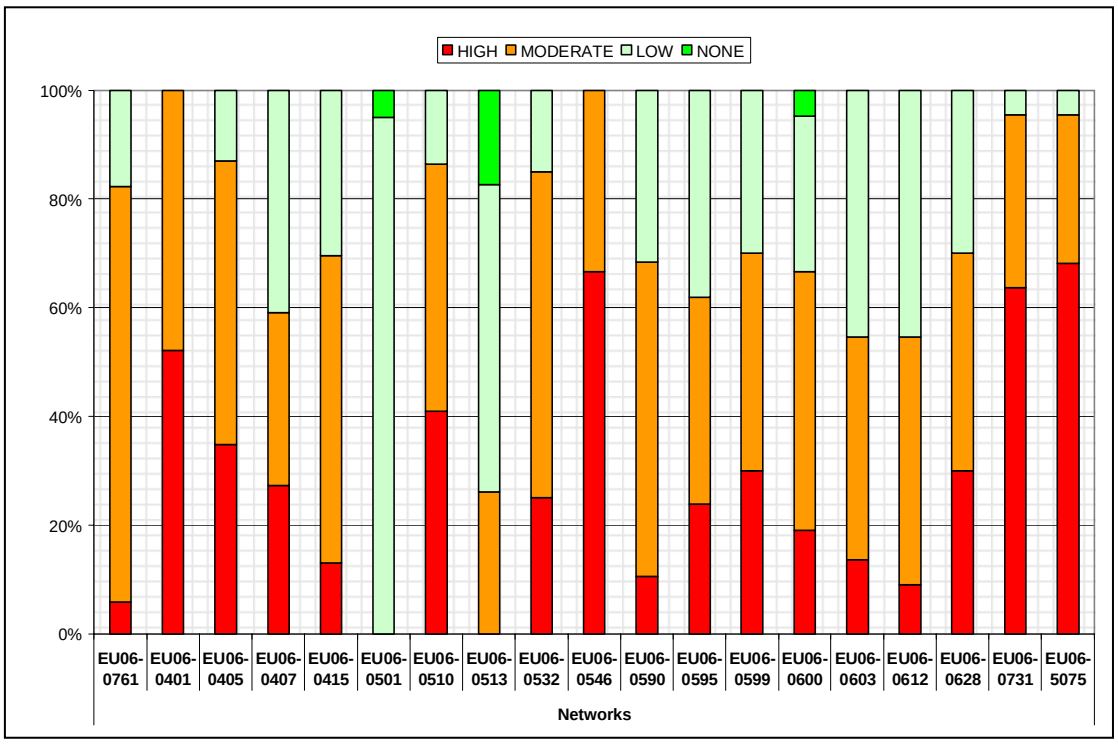


Figure 4: Example - Analysis of Cost to Implement

Risk to Not Implement

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

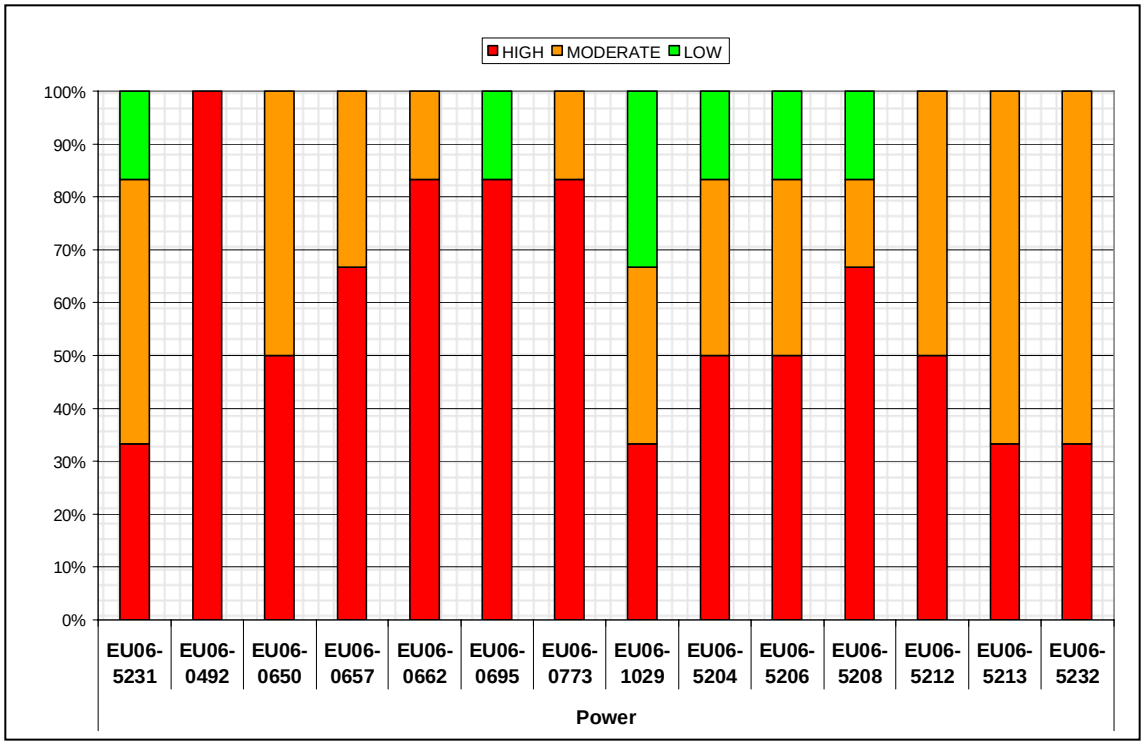


Figure 5: Example – Analysis of Risk to NOT Implement

Level of Implementation

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

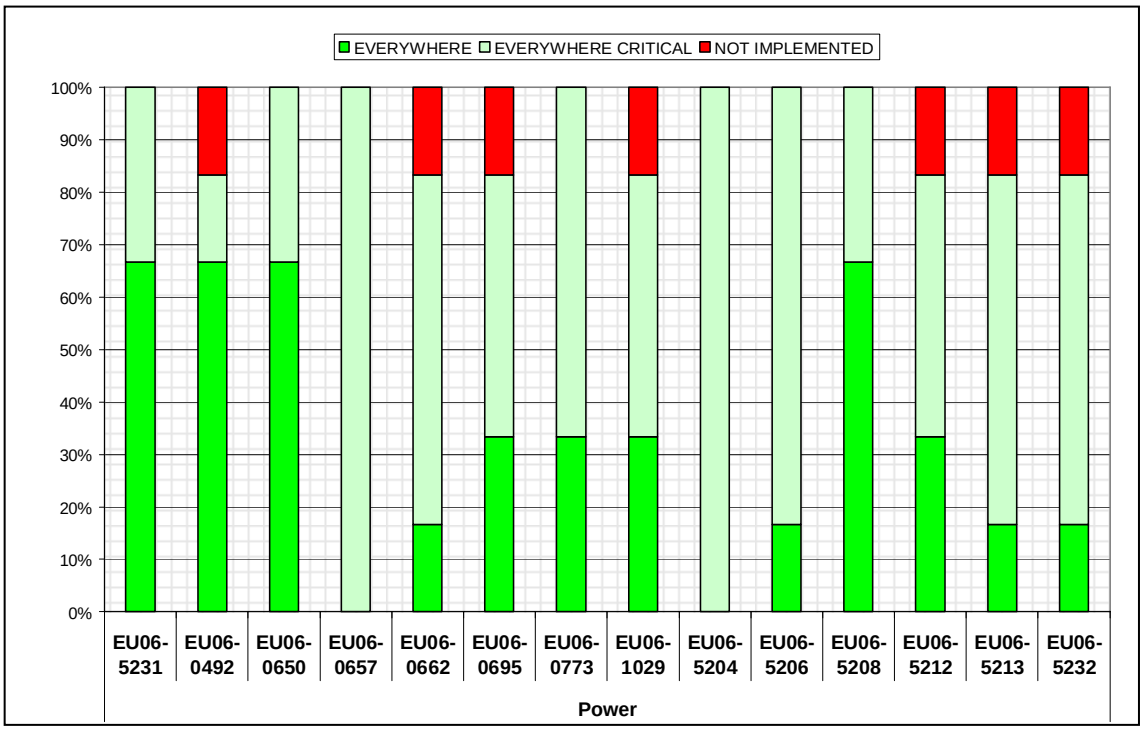


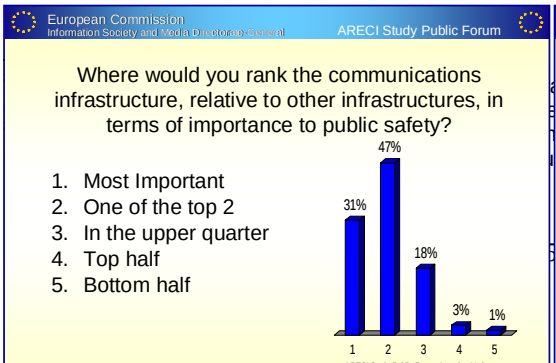
Figure 6: Example – Analysis of Level of Implementation

2.5.4 Public Forum

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

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

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



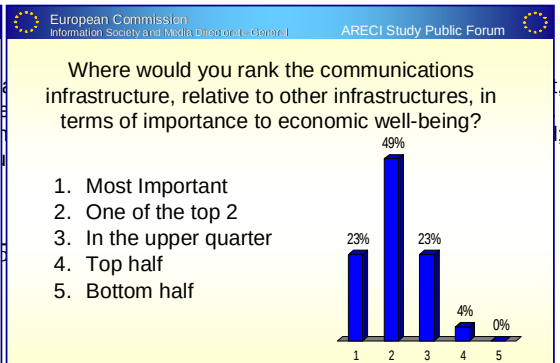


Figure 7: Public Forum Stakeholder Voting on Communications Infrastructure

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

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

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

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

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

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

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

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

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

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

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

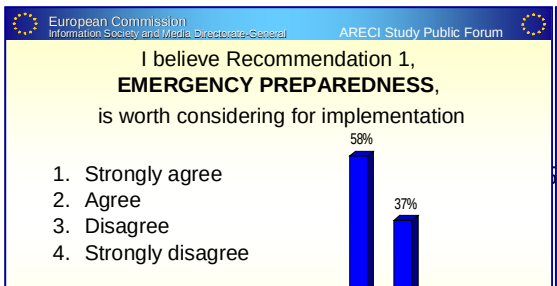


Figure 8: Public Forum Stakeholder Voting on Recommendations

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

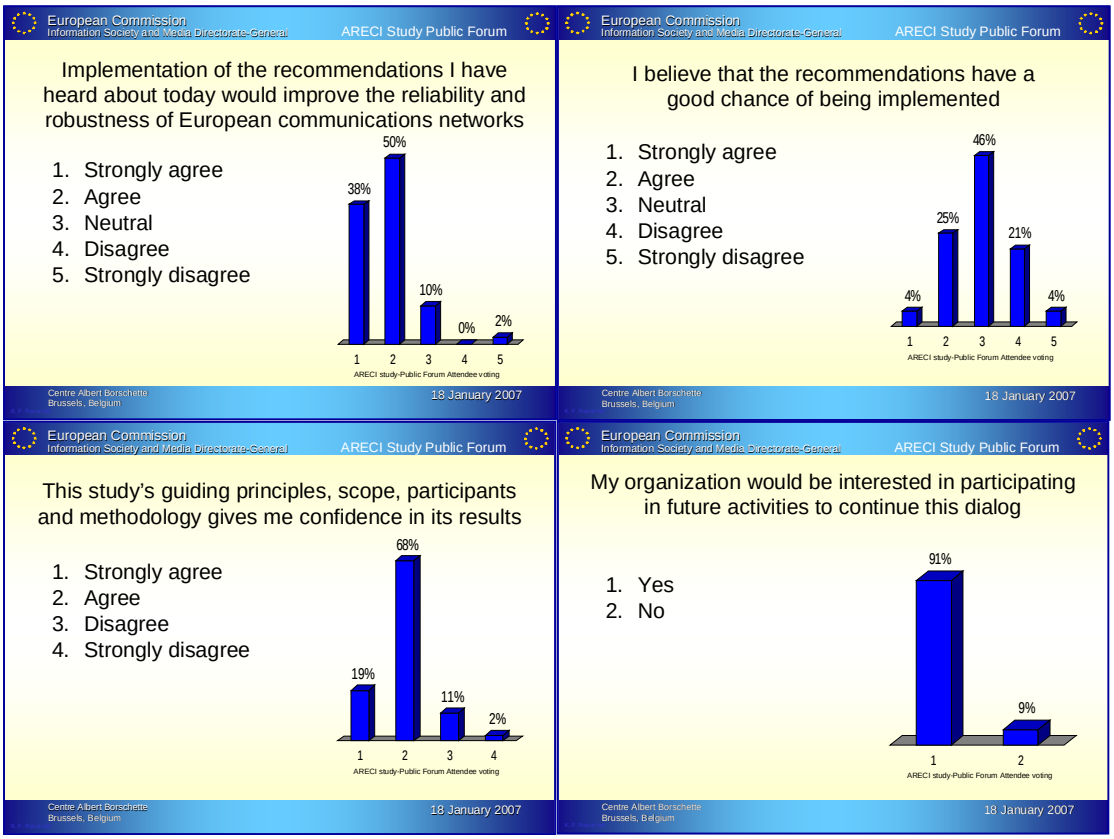


Figure 9: Public Forum Stakeholder Summary Voting

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

organisation would be interested in participating in future activities to continue the dialog.[25]

2.6 Recommendation Development

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

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

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

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