Chapter 1

THE EUROPEAN PERSPECTIVE OF TELECOMMUNICATIONS AS A CRITICAL INFRASTRUCTURE

Fabio Bisogni, Simona Cavallini, Luisa Franchina, and Giovanni Saja

Abstract This paper attempts to analyze the degree to which the telecommunications sector is regarded as a critical infrastructure at the European level. Taking into account a new categorization of telecommunications applications and infrastructure perspectives, a new matrix-based classification method is proposed to clarify the protection approaches of policy makers and telecommunications asset owners and operators. The so-called "criticality matrix" approach applied to the Italian environment demonstrates the different perspectives held by policy makers and telecommunications asset owners and operators, and shows how all the stakeholders may engage a common base to define efficient and effective strategies that can enhance the security and resilience of critical infrastructure assets.

Keywords: Europe, critical infrastructures, telecommunications, classification

1. Introduction

The importance of telecommunications to all the societal sectors has led European policy makers to include it in the list of potential critical infrastructures. This view is also corroborated by research on interdependencies between critical infrastructures and the consequent cascading effects of telecommunications failures (see, e.g., [1, 16–18]). Interested readers are referred to Luiijf, *et al.* [15] for an analysis of the interdependencies involving the telecommunications sector and other European critical infrastructure sectors.

In June 2004, the European Council requested that a comprehensive strategy be created for protecting critical infrastructures. In October 2004, the European Commission adopted a communication on critical infrastructure protection as part of the fight against terrorism [5]; this communication included several proposals for enhancing prevention, preparedness and response at the

J. Butts and S. Shenoi (Eds.): Critical Infrastructure Protection VI, IFIP AICT 390, pp. 3–15, 2012.

European level in the event of terrorist attacks on critical infrastructure assets. In December 2004, the Council, in its conclusions on prevention, preparedness and response to terrorist attacks, approved the European Commission's proposal to establish a European Programme for Critical Infrastructure Protection (EPCIP) that would spearhead various initiatives aimed at enhancing critical infrastructure protection.

The next year, in November 2005, the European Commission adopted a "green paper" [7] that outlined strategic alternatives with regard to critical infrastructure protection. The process culminated with a 2008 European Council directive that emphasized the identification and designation of European critical infrastructures and an assessment of the need to improve their protection [12].

Recognizing the existence of several infrastructures whose disruption or destruction could have a significant impact on member states, the European Council directive focused on clarifying the key elements related to critical infrastructure protection. In particular, the directive defined the following key concepts:

- **Critical Infrastructure:** Assets, systems or parts thereof located in European Union member states, which are essential for the maintenance of vital social functions, security, safety, health and economic/social welfare of the population, and whose destruction or malfunction would have a significant impact in a member state (loss of service).

- **European Critical Infrastructure:** Critical infrastructures located in European Union member states whose destruction or malfunction would have a significant impact in at least two European Union member states. The significance of the impact is to be assessed in terms of cross-cutting criteria, including the effects of cross-sector dependencies on other infrastructures.

The directive also defined a common approach for identifying European critical infrastructures and protecting them. Since the various sectors have accumulated extensive expertise and experience with regard to asset protection, the directive was designed to be implemented on a sector basis. At this time, two areas – energy and transportation and their related sub-sectors – are identified by the directive as domains in which the procedures for identifying European critical infrastructures must be applied.

The implementation of the directive has imposed a number of requirements on member states that impact the activities and organization of owners and operators of the identified European critical infrastructure assets. In particular, the identification of a European critical infrastructure on the part of a member state leads to a procedure with two requirements for asset owners and operators:

- **Implementation of Operator Security Plans:** The directive provides an indication of the minimum components that must be addressed in a plan. In particular, a plan should identify the critical infrastructure

assets and the security solutions that are in place and those that are being implemented. Also, the procedures should cover, at the very least: the identification of critical assets; a risk analysis that includes threats, vulnerabilities and potential impacts; the identification, selection and prioritization of countermeasures, categorized as those that are permanent and those that are enforceable gradually.

- **Appointment of Liaison Officers:** The directive requires liaison officers to act as a points of contact between the critical infrastructures and the national bodies responsible for their protection.

The 2008 directive also recognized the future need to expand the list of critical infrastructures. Indeed, it gave priority to the information and communications technology sector during the first review, which started in January 2012.

Following the 2008 directive and its goal of increasing the scope of the European critical infrastructure sectors, the European Commission issued a 2009 communication to protect Europe from large-scale cyber attacks and disruptions, and enhance preparedness, security and resilience [9]. This communication articulated European policy on strengthening security and trust in the information society. Focusing attention on prevention, preparedness and awareness, it specified immediate actions to strengthen the security and resilience of critical information and communication infrastructures, including all aspects of telecommunications services. Subsequent European Union debate spurred efforts to examine the challenges and priorities for network and information security policy and to set up the most appropriate instruments needed at the European level to ensure the security and resilience of critical information nfrastructures.

The 2009 communication on critical information infrastructures came at the end of a process extending back to 2005 that focused on the increasing role of the telecommunications sector in Europe. A 2005 Commission communication [6] highlighted the urgent need to coordinate efforts to build the trust and confidence of stakeholders in electronic communications and electronic services. To this end, a strategy for a more secure information society was adopted in 2006 [8]. This 2006 communication was produced to revitalize the European Commission strategy set out in 2001. The main intent was to develop a dynamic, global strategy in Europe, based on a culture of security and founded on three pillars: dialogue, partnership and empowerment. As part of the partnership framework, the 2006 communication asked the European Network and Information Security Agency (ENISA) to develop a trusted partnership with member states and stakeholders to develop an appropriate data collection framework, including procedures and mechanisms to collect and analyze European-Union-wide data on security incidents and consumer confidence. Member states, the private sector and the research community are required to establish strategic partnerships to ensure the availability of data on the information and communications technology security industry and on market trends for products and services in the European Union (EU). Moreover, to improve the ability to

respond to network security threats, the European Commission asked ENISA to examine the feasibility of a European information sharing and alert system to articulate effective responses to current and emerging threats.

The 2006 communication sought to achieve the infrastructure identification and protection objectives by adopting a multi-stakeholder approach and promoting effective public policy and private sector initiatives. According to this goal, in order to identify the key assets in the telecommunications sector and to adequately protect them, the relevance of the perspectives adopted by European and national policy makers should match the organizational approach of telecommunications operators in meeting their security and resilience requirements. Indeed, what is needed is a common framework in terms of approaches and goals that would support efficient and effective security and resilience strategies.

2. European Telecommunications Sector

The first step in developing a common framework for policy makers and asset owners and operators is to define the components of the telecommunications sector regardless of the geographic areas in which they are located. At present, statistics on the evolution of telecommunications markets are becoming wide and consistent, thanks to the efforts of several governmental and non-governmental organizations.

The availability of public data related to the larger information and communications technology sector is relatively broad. The primary reliable sources for the European context are Eurostat, Organization for Economic Cooperation and Development (OECD) and International Telecommunications Union (ITU). These entities conduct electronic and postal surveys as well as interviews at the national and international levels in order to obtain high-quality statistical data. The resulting data can be used to define indicators that are comparable across countries. However, limited data is available about telecommunications applications and usage.

Using the traditional classification of telecommunications applications in terms of fixed telephony, mobile telephony and Internet, the first point of reference is Eurostat, which, through the national statistical institutes, provides an annual dataset on the twenty-seven EU member states (EU-27). Information and communications technology market features are clarified through statistics that link telecommunications and various economic indicators of the member states.

A valuable Eurostat data asset is the elaboration of several aggregate indicators such as "Internet activities of enterprises." However, as far as telephony is concerned, data is provided in terms of the volume of different types of calls along with indicators related to operators and service providers. Eurostat data sources are also useful for analyzing information and communications technology use by citizens. Indeed, various statistics are available about the expanding role of information and communications technology in daily activities, especially related to "households" and "individuals." Several indicators pertaining

to network access also give a good sense of the importance of telecommunications services.

OECD databases and statistics are also valuable sources of information about the telecommunications sector. The available data includes communication channel access (fixed, mobile and Internet), employees, revenue, capital and investment. The main limitations of OECD data related to the European telecommunications sector are that they cover only part of the EU-27 and that most OECD statistics are published in books instead of being disseminated free of charge on the Internet. Nevertheless, the OECD Directorate for Science Technology and Industry frequently publishes some information and communications technology indicators from its various databases. These indicators cover trade, firms, use and growth related to information and communications technologies.

ITU, the U.N. telecommunications agency, maintains a highly reliable and often quoted database that contains data provided directly by governments via ITU's annual questionnaires. Data related to the telecommunications sector, which is available on a payment basis, cover more than 200 countries, including all the EU-27 countries from 1960 onwards. The data related to fixed and mobile telephony includes coverage, diffusion, traffic, prices, revenues and investments. The same data is also available for the entire telecommunications sector with the addition of some data about faults. In the case of the Internet, the available data primarily focuses on the numbers of users and subscribers.

Another reliable, but limited, data source is the annual report prepared by the European Telecommunications Network Operators Association (ETNO). The report provides data about the European telecommunications market for fixed telephony, mobile telephony and Internet, focusing mainly on operator revenue trends and ETNO member investments.

3. Infrastructure Approach

At the European level, telecommunications is considered to be a complex critical infrastructure sector. Also, national approaches and related regulations hinder a common approach – in the member states, the criteria for identifying critical infrastructures are defined by various *ad hoc* public institutions and government entities.

Most European member states use the following approaches when defining and identifying critical infrastructures:

- **Service-Oriented Approach:** This approach focuses on the services and/or functions that are vital to society. Infrastructures that provide these services and/or functions are considered to be critical infrastructures.

- **Asset-Oriented Approach:** This approach focuses on the impact and/or risk. Infrastructures whose disruption may result in major impact in terms of casualties, economic and public effects are considered to be critical infrastructures.

- **Operator-Oriented Approach:** This approach focuses on infrastructure operators because of their decision-making roles in providing vital services. Operators are considered critical on the basis of legislative obligations and spontaneous interactions because they help ensure the protection of assets and the resilience of services.

A 2011 study by IABG, Booz and Alcatel-Lucent [13] investigated the sectoral criteria for identifying European critical infrastructures. The study involved sixteen European countries and incorporated contributions by 68 organizations, mainly national entities with information and communications technology responsibilities and telecommunications operators. According to the study, most of the member states are considering the information and communications sector as outlined in Directive 2008/114/EC [12]. About two-thirds of the member states adopt the service-oriented approach (or its variations) in designating critical infrastructures, while just a few countries engage the asset-oriented approach or the operator-oriented approach. In some limited cases, critical infrastructures are identified based on common aspects of all three approaches.

4. Proposed Classification Method

The aforementioned 2009 European Commission communication [9] encourages member states to continue to develop, in cooperation with all relevant stakeholders, criteria for identifying critical infrastructure assets in the information and communications technology sector. According to many experts, the main obstacle to applying the criteria promoted by the European critical infrastructure directive [12] is the nature of the information and communications technology sector and the telecommunications component. Information and communications technology has a strategic role because it pervades all societal activities, but its horizontal nature prevents precise boundaries from being defined for the sector.

For this reason and others, a classification method for identifying the criticality of the telecommunications infrastructure should rely on a multi-faceted framework that is shared among the main stakeholders of the sector. Because of the quality of service and the security and resilience provisions, two dimensions must be considered: (i) telecommunications applications; and (ii) the adopted infrastructure approach.

The first dimension of the proposed classification method is telecommunications applications. The traditional classification of telecommunications applications as fixed telephony, mobile telephony and Internet is gradually losing its significance as a result of service convergence and communication channel integration. Although the main statistics in the telecommunications sector are collected using the traditional classification, the evolution of technologies as connected software, hardware and middleware suggests that a content-oriented taxonomy would be more appropriate. Therefore, our proposed method classifies telecommunications applications in terms of voice communications, data

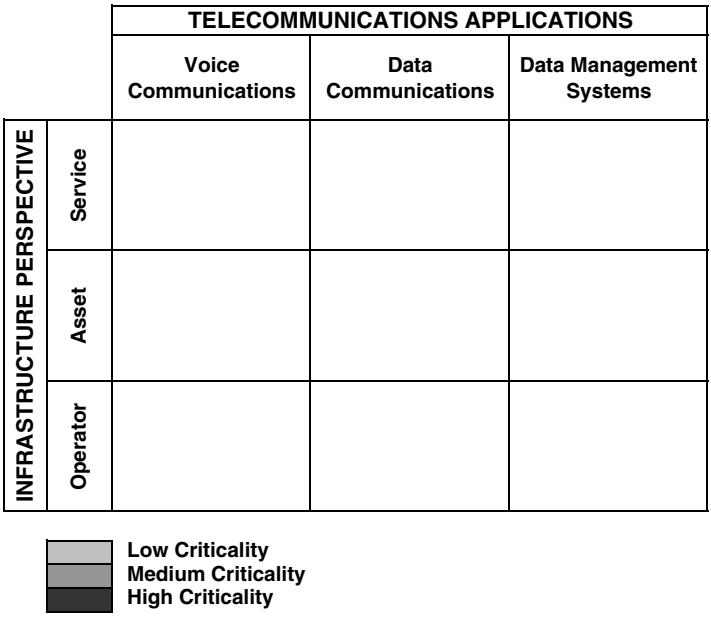

Figure 1. Classification matrix.

communications and data management systems (i.e., data processing, hosting and related activities).

The second dimension of the proposed classification method is the adopted infrastructure approach, which may be service-oriented, asset-oriented or operator-oriented. According to this dimension, the provided services (e.g., fixed telephony), essential assets (e.g., public switched telephone network facilities) and operators (e.g., Telecom Italia) are all infrastructure objects with security and resilience provisions.

The classification matrix presented in Figure 1 allows the various telecommunications sector stakeholders to define relative criticality levels (low-level, medium level and high-level) based on the appropriate thresholds. The matrix can be used to compare the frames of reference used by policy makers (e.g., national authorities) and owners and operators of potential critical information infrastructure assets (e.g., telecommunications operators) when defining policies and strategies for security and resilience.

5. Italian Case Study

This section presents a case study where the classification methodology described in the previous section is applied to the Italian telecommunications sector.

Table 1. Total expenses per operator in Italy in 2009 and 2010 [14].

Operator	2009	2010
Telecom Italia	**51.6%**	**48.9%**
Vodafone Italia	20.6%	21.4%
Wind	12.5%	13.6%
Fastweb	4.6%	4.9%
H3G	3.7%	4.2%
BT Italia	2.8%	2.7%
Others	4.3%	4.4%
Total	**100.0%**	**100.0%**

5.1 Italian Telecommunications Sector

According to the implementation of Article 53 of the Italian Legislative Decree on the Electronic Communication Code (CCE) of August 1, 2003, all users within the national boundaries, regardless of their geographical locations, should be able to access "universal communication services" at a pre-defined quality level. In addition, telecommunications companies must provide these universal communication services to all users at an affordable price.

At present, Telecom Italia is Italy's only unique provider of universal communications services. According to Article 54 of CCE, Telecom Italia must provide fixed telephony services in addition to free emergency services. With regard to security and resilience, specific quality targets for fixed telephony services related to the line disruption rate and recovery time were initially regulated by Article 61, but have been updated in recent years. These indications match the findings of the 2011 study by IABG, Booz and Alcatel-Lucent [13], which noted that Italy tends to uses the service-oriented approach for identifying critical information infrastructures.

Telecom Italia's position as the leading Italian telecommunications provider has historical roots. Telecom Italia was established in 1994 as result of the merger of STET and SIP, which was the only Italian telecommunications company since 1964. It was not until 1997 that the Italian telecommunications market was opened to other national and international operators in the fixed telephony, mobile telephony and Internet sub-sectors. In 2010, at least six operators provided both fixed and mobile telephony to the Italian market. However, according to the latest (2010) data in Table 1, Telecom Italia is the largest in terms of expenses for fixed and mobile telephony (48.9%). The other main players are Vodafone Italia (21.4%) and Wind (13.6%).

Using a sub-sector classification similar to the traditional classification, the market shares of fixed telephony connections and bandwidth connections also show the dominance of Telecom Italia (Table 2). However, Vodafone Italia is the principal provider of mobile telephony services.

Table 2. Market shares of Italian telecom operators in 2010 [14].

Operator	Fixed Connections[1]	Bandwidth Connections[1]	Mobile Voice and Data
Telecom Italia	**71.6%**	**53.9%**	35.7%
Vodafone Italia	7.4%	12.0%	**36.8%**
Wind	10.6%	14.8%	18.4%
Fastweb	7.5%	12.9%	NA[2]
H3G	NA[2]	NA[2]	7.2%
BT Italia	0.4%	0.9%	NA[2]
Tiscali	1.9%	4.1%	NA[2]
Others[3]	1.4%	13.6%	1.9%
Total	**100.0%**	**100.0%**	**100.0%**

[1] December 2010 data.
[2] Operator does not provide the service or its market share is included in Others.
[3] Includes mobile virtual network operators for mobile telephony.

5.2 Telecom Italia

Telecom Italia is the largest Italian provider of fixed telephony services. It is a major international player with 57,853 employees in Italy and a total of 84,335 people worldwide (according to the 2011 corporate report). In 2010, the company had industrial investments of 4,583 million euros, turnover of 27,571 million euros and earnings before interest, taxes, depreciation and amortization (EBITDA) of 11,412 million euros.

The domestic (Italian) infrastructure of Telecom Italia includes 31.3 million mobile telephony lines (Telecom Italia Mobile), 9.1 million broadband connections (1.9 million of them wholesale costumers) and 15 million retail fixed line connections (7.2 million of them broadband connections).

The international operations of Telecom Italia are primarily focused on South America: 55.5 million mobile lines in Brazil (25.5% share); 17.4 million mobile lines, 4.1 million fixed lines and 1.5 million broadband connections in Argentina; and 2 million mobile lines in Paraguay.

With regard to Telecom Italia, the definition of infrastructure criticality is essential in order to apply the mandated security and resilience measures. As the main Italian company, Telecom Italia is regarded by the Italian Government as the owner and operator of a potential critical infrastructure, and the operator-oriented approach is applicable because of Telecom Italia's role as the sole provider of universal communications services.

However, in order to guarantee the protection of the telecommunications infrastructure, a strong asset-oriented perspective is adopted internally by Telecom Italia. Assets are defined as those that are physical and substantial. The criticality of the assets is determined by a three-step process: defining the asset boundaries, assessing the quality of the provided services and guaranteeing the

level of user satisfaction. Taking into account these three connected aspects, the criticality depends on the weakest link in the chain. Thus, a critical infrastructure can be considered to be an asset that makes a service available, and the absence of the service produces significant disruptions for end users. For this reason, the criticality lies in "transporting" the service to end users.

For security and resilience purposes, identifying assets and the related processes of service production and delivery are crucial. The optimal solution is a homothetic organization. Each structure in such an organization has its own responsibilities, updates the risk map, sets up operator security plans, defines recovery and continuity plans, and guarantees the compliance of the implemented activities in order to avoid functional overlap.

The Telecom Italia approach involves defining the asset boundaries and assessing the criticality of the assets. Producing an exhaustive and unambiguous list of assets supports the identification of the key elements that are required to deliver services (business processes, technological functions, human resources, facilities, etc.). The vulnerabilities and related risks are evaluated for each asset by applying heuristic techniques (e.g., a quasi-logarithmic scale) because the probabilities of occurrence of rare and high-impact critical events are usually not available. This technique, which is based on a non-linear scale, ensures more precise evaluations because it highlights the exceptional occurrence of minimum and maximum values.

The computation of the expected impact as a score for each location in terms of vulnerability multiplied by risk allows a ranking of the criticality of the locations themselves. A logarithmic ranking of locations and their assets is then created according to different levels of criticality. The logarithmic ranking assists in separating critical assets from less strategic assets. Having a smaller number of critical assets also helps focus protection efforts.

Based on this approach, Figure 2 shows the criticality matrix classification results for Telecom Italia. From the service perspective, voice communications, which is related to fixed telephony and has special regulatory attention, is not ranked as the application with the highest criticality. However, from the asset-oriented perspective, data management systems has the highest criticality.

The proposed classification method has two main benefits. The first benefit is the opportunity to increase stakeholder awareness about the criticality of the telecommunications infrastructure according to different perspectives while also enabling the comparison of infrastructure criticality. In fact, during the course of the case study, Telecom Italia had to reason about its perspective with regard to managing criticalities and about the perspectives adopted by other stakeholders, including policy makers and competitors.

The second benefit is policy making support. The criticality matrix summarizes certain structural features of the telecommunications framework such as the influence of legal provisions (e.g., regarding the universal communications services provided by Telecom Italia) and the direct liability of the telecommunications infrastructure (e.g., ownership of the physical infrastructure, especially fixed telephony).

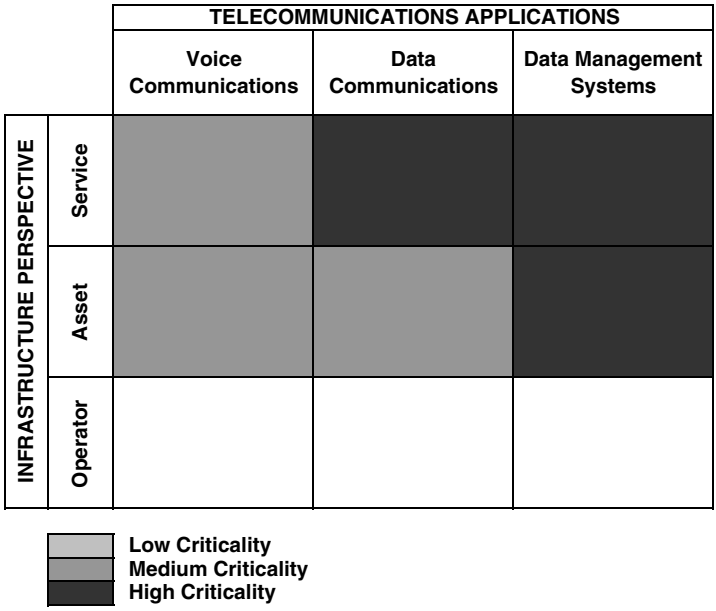

Figure 2. Classification method applied to Telecom Italia.

Thus, the criticality matrix method provides a homogeneous classification. In particular, it enables the various stakeholders to assess the criticality of telecommunications applications according to the specific infrastructure perspectives they adopt. Note, however, that in order to enhance the utility of the classification method, it is recommended to collect and use data based on the three types of telecommunications applications shown in Figure 2.

6. Conclusions

The growing societal reliance on the telecommunications sector has made it imperative to ensure that the critical information and communications infrastructure is secure and resilient. While there is broad agreement on the need to protect critical infrastructures, different perspectives and approaches are applied at the European level to identify – and ultimately protect – infrastructure assets. This heterogeneity has driven the effort to develop the criticality matrix classification method. The method offers a common, shared framework for policy makers and asset owners and operators to identify key infrastructure assets and to assess their criticality, helping formulate effective and efficient security and resilience strategies. The Telecom Italia case study demonstrates the different perspectives and decision processes that can be applied to identify infrastructure assets and assess their criticality; and how the criticality matrix method can be used to provide a highly homogeneous classification that

also facilitates the comparison of results obtained using different infrastructure perspectives.

References

[1] F. Bisogni and S. Cavallini, Assessing the economic loss and social impact of information system breakdowns, in *Critical Infrastructure Protection IV*, T. Moore and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 185–198, 2010.

[2] F. Bisogni, S. Cavallini, R. Bellotti, M. Tancioni, L. Remotti, A. Wright, G. Gasperini and S. Anselmucci, The Vulnerability of Information Systems and its Inter-Sectoral, Economic and Social Impacts – VIS, Final Project Report, Formit Foundation, Rome, Italy, 2009.

[3] S. Cavallini, S. Di Trocchio, F. Bisogni, M. Tancioni and P. Trucco, Development of a Methodology and Research of Quantitative Data on the Economics of Security and Resilience in Critical Communications and Information Infrastructures – SMART-SEC, Final Project Report, Formit Foundation, Rome, Italy, 2010.

[4] European Commission, Network and Information Security: Proposal for a European Policy Approach, Commission Communication COM(2001) 298, Brussels, Belgium, 2001.

[5] European Commission, Critical Infrastructure Protection in the Fight Against Terrorism, Commission Communication COM(2004) 702 Final, Brussels, Belgium, 2004.

[6] European Commission, A European Information Society for Growth and Employment, Commission Communication COM(2005) 229 Final, Brussels, Belgium, 2005.

[7] European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, Commission Communication COM(2005) 576 Final, Brussels, Belgium, 2005.

[8] European Commission, A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment, Commission Communication COM(2006) 251, Brussels, Belgium, 2006.

[9] European Commission, Protecting Europe from Large-Scale Cyber Attacks and Disruptions: Enhancing Preparedness, Security and Resilience, Commission Communication COM(2009)149 Final, Brussels, Belgium, 2009.

[10] European Commission, A Digital Agenda for Europe, Commission Communication COM(2010) 245, Brussels, Belgium, 2010.

[11] European Parliament and Council, On a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), Directive 2002/21/EC, Brussels, Belgium, 2002.

[12] European Parliament and Council, On the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, Directive 2008/114/EC Brussels, Belgium, 2008.

[13] IABG, Booz and Alcatel-Lucent, Study to Support the Process to Define Sectoral Criteria to Identify European Critical Infrastructures in the ICT Sector, with Particular Focus on the Sub-Sectors of Internet, Fixed and Mobile Telecommunications, Final Project Report, Ottobrunn, Germany, 2011.

[14] Italian Authority for the Protection of Communications (AGCOM), Relazione Annuale 2011 sull'Attivita svolta e sui Programmi di Lavoro (in Italian), Naples, Italy (`www.agcom.it/Default.aspx?message=downloadpdf&DocID=131`), 2011.

[15] E. Luiijf, A. Nieuwenhuijs, M. Klaver, M. van Eeten and E. Cruz, Empirical findings on critical infrastructure dependencies in Europe, *Proceedings of the Third International Workshop on Critical Information Infrastructure Security*, pp. 302–310, 2009.

[16] P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, Technical Report INL/EXT-06-11464, Idaho National Laboratory, Idaho Falls, Idaho, 2006.

[17] J. Santos and Y. Haimes, Modeling the demand reduction input-output inoperability due to terrorism of interconnected infrastructures, *Risk Analysis*, vol. 24(6), pp. 1437–1451, 2004.

[18] J. Sarriegi, F. Sveen, J. Torres and J. Gonzalez, Adaptation of modeling paradigms to the critical infrastructure interdependencies problem, *Proceedings of the Third International Workshop on Critical Information Infrastructure Security*, pp. 295–301, 2009.