Security and Protection of Critical Infrastructures: A Conceptual and Regulatory Overview for Network and Information Security in the European Framework, also focusing upon the Cloud Perspective

Ioannis P. Chochliouros
Research Programs Section Fixed,
OTE (Hellenic Telecommunications
Organization S.A.)
1, Pelika & Spartis Str.
GR-15122 Maroussi, Greece
+30-210-6114651
ichochliouros@oteresearch.gr

Anastasia S. Spiliopoulou
OTE
(Hellenic Telecommunications
Organization S.A.)
99, Kifissias Avenue
GR-15124, Athens, Greece
+30-210-6115112
aspiliopoul@ote.gr

Ioannis M. Stephanakis
OTE
(Hellenic Telecom Organization S.A.)
99, Kifissias Avenue
GR-15124, Athens, Greece
+30-210-6116798
stephan@ote.gr

Dimitrios N. Arvanitozisis
OTE
(Hellenic Telecommunications
Organization S.A.)
99, Kifissias Avenue
GR-15124, Athens, Greece
+30-210-6335613
darvanito@ote.gr

Evangelos Sfakianakis
Maria Belesioti
Evangelia Georgiadou
Research Programs Section Fixed,
OTE (Hellenic Telecommunications
Organization S.A.)
1, Pelika & Spartis Str.
GR-15122 Maroussi, Greece
+30-210-6114938
{esfak, mbelesioti,
egeorgiadou}@otersearch.gr

Nina Mitsopoulou
OTE
(Hellenic Telecommunications
Organization S.A.)
99, Kifissias Avenue
GR-15124, Athens, Greece
+30-210-6111536
nmitsopoulou@ote.gr

ABSTRACT

In the concept of the present work we intend to identify the importance for the promotion, the establishment and the effective development of suitable measures towards protecting and supporting modern critical infrastructures (CIs), as the latter compose essential parts of our modern societies and economies. Thus, we first discuss and analyze, *in depth*, the necessary conceptual definitions together with all related policy initiatives and other potential corresponding approaches globally, but by putting particular emphasis upon the actual European environment. As CIs are fundamental elements -or modules- for growth and development, the modern European strategy framework implicates for suitable measures to be applied to adequately fulfil that purpose, in particular for assessing any potential risks that may be harmful for the proper functioning -or even for the viability- of such important infrastructures. Then, we focus our concerns upon the exact context implicated by the present multi-faced challenges for ensuring an appropriate level of network and information security (NIS) and protection within the broader CI environment. In fact, we discuss in detail and also we assess a wide variety of issues affecting the proper role of IT tools and of related facilities, in general, as an indispensable part of the CI protection in the modern EU policy. Then, we concentrate upon the option of properly considering the cloud as a means for supporting IT relevant to serve CI protection. Under the innovative features introduced by the innovations promoted by cloud computing, related opportunities are also discussed, together with associated threats. Critical infrastructure providers have stringent security assurance and resilience requirements that reflect business, regulatory and legal obligations. To ensure these are properly met when providers use the cloud, techniques for assurance evaluation have to be produced. In this context we also refer to the specific initiatives structured and developed within the scope of the EU-funded SECCRIT research program that promote a first significant attempt to deal with that major challenge.

Categories and Subject Descriptors

• **Networks~Network properties.** Network and information security.

• **Networks~Distributed architectures.** Cloud computing.

• **Security and privacy~Intrusion/anomaly detection and malware mitigation.** Cloud computing.

• **Social and professional topics~Computing and technology policy.** Privacy policies.

16th EANN workshops, September 25 - 28, 2015, Rhodes Island, Greece.
© 2015 ACM. ISBN 978-1-4503-3580-5/15/09…$15.00
DOI: http://dx.doi.org/10.1145/2797143.2797146.

Keywords

Critical Infrastructure (CI); Critical Infrastructure Protection (CIP); Critical Information Infrastructure (CII); Cloud Computing; European Critical Infrastructure (ECI); Legal European Framework; Network and Information Security (NIS); Resilience; Security.

1. INTRODUCTION – ESSENTIAL CONCEPTUAL FRAMEWORK

Under the term **"critical infrastructure (CI)"** is conceived a particular asset or a system which is necessary for the maintenance and the continuity of vital societal functions [1]. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviours, may have an important negative impact for the security of the EU and the well-being of its citizens. The term "infrastructure" usually describes the underlying basis of an organization or system, for example, a country and includes, in principle: Information and telecommunications systems; banking and financial institutions; water, electricity, oil and gas supplies; transportation and logistics structures; and health and emergency services. In addition, the word "critical" is more appropriate than "infrastructure" for making a conceptual distinction between normal operating procedures and strategic security policy.

Reducing the vulnerabilities and the weaknesses of CI and rising their resilience is one among the well-defined objectives of the EU policy. An acceptable level of protection has to be provided and the harmful effects of disruptions on the society and upon the involved citizens need to be reduced, *to the extent possible*.

According to the European policy context, critical infrastructures comprise those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a severe impact and influence on the health, safety, security or economic well-being of citizens or the effective functioning of European or local governments. There are, in fact, three types of corresponding infrastructure assets:

• Public, private and governmental infrastructure assets and interdependent cyber & physical networks.

• Procedures and -where relevant- individuals that exercise control over critical infrastructure functions and/or operations.

• Objects having cultural or political significance as well as "soft targets" which may also incorporate mass events (i.e. sports, leisure and cultural).

Following to the previous more "generalised" concept as discussed above, the term **European Critical Infrastructure (ECI)** implies those specific physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more Member States (MS) [2]. The pure definition of *"what may constitute an EU critical infrastructure"* is given by its cross-border effect which ascertains *whether an incident could have a serious impact beyond two or more MS national territories*. This is conceived as the loss of a critical infrastructure element and is rated by the: (i) Extent of the geographic area which could be affected by the loss or unavailability of a critical infrastructure element beyond three or more Member State's national territories; (ii) effect of time (i.e. the fact that a for example a radiological cloud might, with time, cross a border), *and;* (iii) level of the so-called interdependency. ("*Interdependency"* [3] is a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other; *for example, an electricity network failure in one MS affecting another).* According to the approach suggested in [2], there are four types of interdependencies for critical infrastructures: (i) Physical: the operation of one infrastructure depends on the material output of the other; (ii) Cyber: dependency on information transmitted through the information infrastructure; (iii) Geographic: dependency on local environmental effects simultaneously affecting several infrastructures, and; (iv) Logical: any kind of dependency not characterized as Physical, Cyber or Geographic.

According to the context of the ***Council Directive 2008/114/ EC***, an EU critical infrastructure is an "asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".

The scope of that Directive was originally limited to the energy and transport sectors. However, it has constituted the "first step" in a step-by-step approach to detect, identify and then designate ECIs and assess the need to improve their protection. The Directive outlined the approach all Member States would be required to follow to identify, designate, and protect ECIs in the energy and transport sectors, while indicating the ICT sector as a priority for possible future expansion of its scope. The majority of Member States have implemented the provisions of this Directive by incorporating them within their national legislative and regulatory frameworks through a variety of approaches.

As previously mentioned, CI can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. To save the lives and property of citizens being at any kind of potential risk in the EU territory from terrorism [4], natural disasters and accidents, any disruptions or manipulations of CI should, *to the extent possible*, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States, their citizens and the European Union [5].

The effective CI protection implies a proper level communication, coordination, and cooperation nationally and at EU level among all interested parties, including: the owners and operators of infrastructure (the latter are entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part of these), regulators, professional bodies and industry associations in collaboration with all other sectors of government, and the wider public.

Critical Infrastructure Protection (CIP) is about ensuring that services vital to the society continue to function even after the occurrence of any harmful event [6]. It also implicates the capability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction, when some of these may appear and threaten the proper operation of the corresponding asset [7]. In particular, the general objective of CIP in the EU is to raise critical infrastructure protection capabilities across all EU Member States against all possible hazards. The underlying rationale is that disruption to infrastructures providing key services could harm the security and economy of the EU as well as the well-being of its citizens and so it is essential to work for proper prevention and/or counter measures.

The term **"Critical Information Infrastructure (CII)"** refers to all ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, fibre optics, etc.). These infrastructures are necessary for the correct operation of most other CIs and compose a vital tool for managing risk factors and for "returning infrastructures to order" after a breakdown occurs [8].

Critical Information Infrastructure Protection (CIIP) refers to the programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage. Consequently, CIIP has to be assessed as a "cross-sector phenomenon" instead of being restricted to specific sectors. In fact, CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective. This endeavor is a shared responsibility among state, local, tribal, and territorial entities, and public and private owners and operators of critical infrastructure.

By ensuring a high degree of protection of EU infrastructures and increasing their resilience (against all threats and hazards), we can minimise the consequences of loss of services to society as a whole [9]. These objectives feature predominately in the *Stockholm Programme* [10] and in the *EU Internal Security Strategy* [11].

In 2009, the *Stockholm Programme* underlined the importance of critical infrastructure protection by making the need to reduce EU critical infrastructure vulnerabilities one of its objectives. Moreover, the *Stockholm Programme* invited the Council, the Commission, the European Parliament, and the Member States to draw up and implement policies to improve measures for the protection, security preparedness and resilience of critical infrastructure, including Information and Communication Technology (ICT) and services infrastructure. It also called for *Directive 2008/114/EC* to be analysed and reviewed in order to consider including additional policy sectors.

The *EU Internal Security Strategy* highlights that critical infrastructure must be better protected from criminals who take advantage of modern technologies and that the EU should continue to designate critical infrastructure and put in place plans to protect such assets, as they are essential for the functioning of society and the economy. The Strategy also emphasises that the threats to critical infrastructure require enhancements to long-standing crisis and disaster management practices in terms of efficiency and coherence [12]. More specifically, these threats require both solidarity in response and responsibility in prevention and preparedness, with a focus on better risk assessment and risk management [13] of all potential hazards at EU level.

The objective of CI protection at the EU level is to provide satisfactory guarantee that there are adequate and equal levels of protective security on critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements, through the EU [14]. The level of the ensured protection may not be equal for all potential sorts of and can be relevant to the impact caused by the potential failure of the CI. The related European policy and strategy is a continuing process and it so implicates for systematic reviews to identify, assess and consider any new issues and/or related concerns. Furthermore, such actions also have to "minimise" as much as possible any undesirable -or other similar-impact that augmented security investments might have on the competitiveness of a particular industry sector, thus influencing negatively the growth of the European market sector.

Any possible damage of a "part" of infrastructure in one MS may result on quite negative impact or consequences on some others, even potentially affecting the European economy as a whole. This becomes an option of high probability as modern Future Internet (FI)-based technologies and applications are under development, simultaneously with current market liberalisation initiatives in particular for electricity and gas supply) [15]. This context implicates for the development of a commonly accepted framework towards achieving, to the extent possible, **a common level of protection.**

Sufficient protection implicates for communication, coordination, and cooperation nationally, at EU level (*where relevant*) as well as internationally among all stakeholders.

Although man-made threats -and particularly terrorism- is a priority for the EU to deal with [16], the wider concept for a proper CI protection is based on an all-hazards approach. If the level of protective measures in a certain CI sector is found to be as "adequate", then all involved actors-stakeholders concentrate their efforts on threats to which they are vulnerable [17] and look for preventing and corrective measures and policies.

The following **principles** are usually proposed in order to compose the **essential framework for CI protection:**

• ***Subsidiarity*** – This implicates that explicit priority is to be given for the protection of critical infrastructure and that the related action becomes an action of national responsibility. Thus, the national governments need to work together with any involved "market actor" (i.e., owners and/or operators) according to a well-defined and common context. Any relevant cross border issues are to be examined and assessed by the Commission. The actual principle also implicates for responsibility, stability and continuity of all related measures that may be promoted by the market actors, mainly to ensure a proper framework for growth.

• ***Complementarity*** – This implicates that the proposed set of measures and/or actions has to complement any previously existing measures, explicitly or implicitly relevant to the actual ones. In case where there are specific contexts already established and/or validated, these have to remain active in order to support the overall performance of any new action. Complementarity also needs to be ensured with other Community and Union programmes and related initiatives (such as the *European Union Solidarity Fund* and the *Civil Protection Financial Instrument*, the Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions, *Horizon 2020* and the *Structural Funds*).

• ***Confidentiality*** - This implicates that any necessary action for information sharing about CI has to be performed under a framework that provides adequate guarantee about trust and confidentiality. This is an explicit requirement implicating that CIP information has to be classified accordingly and that access has to be granted only on a need-to know" basis. In particular, for the IT sector, an effective information sharing procedure can enable the success of the related sector's public-private partnership model by ensuring that all partners have relevant situational awareness to protect IT and critical functions. Both sharing distribution of relevant kind of information/data entails a relationship of trust such that corporate entities (companies, organisations or any other legal entities) adequately recognize that their sensitive and confidential data will be sufficiently protected, conformant to any requirements set by the European and the national regulatory framework.

• ***Stakeholder Cooperation*** – All stakeholders including the European Authorities, MS, industry and business associations, standardisation bodies and owners, regulators, operators and users ("users" can also involve organizations/legal entities that exploit and use the infrastructure for business and service provision purposes) have a role to play in protecting CI. These actors need to work together so that to be able to effectively contribute to the development, validation and implementation of a modern and efficient EPCIP (European Programme for Critical Infrastructure Protection), according to their specific roles and responsibilities, for the benefit of the entire market and society. In particular, MS authorities have to afford leadership and coordination in developing and implementing a nationally reliable approach to the CI protection within their jurisdictions. On the other hand, the owners, operators and users would be actively involved at both the national and EU level. Where sectoral standards do not exist or where international norms have not yet been established, standardisation organisations could adopt common standards *where appropriate.*

• ***Proportionality*** – Any proposed protection strategies and/or related measures have to be "proportionate" to the level of risk involved as not all infrastructures can be protected from all threats (for example, electricity transmission networks are too large to fence or guard). By applying fitting risk management techniques, priority can be given to those sectors implying for highest risk, by considering the nature of the threat, any comparative criticality, cost-benefit ratio, the level of protective security and the efficiency of existing mitigation strategies. Any proposed actions/measures can be suggested in case where a need has been recognized and assessed, by following an analysis of existing security gaps and this has to be proportionate to the level of risk and type of threat involved.

• ***Sector-by-sector approach*** – As numerous sectors of the market environment already possess specific experience, expertise and requirements with the CIP issue, the corresponding EPCIP has to be built upon an explicit sector-by-sector basis and needs to be implemented by properly following an approved list of CIP sectors.

Prevention implicates the range of deliberate, critical tasks and activities required to shape, sustain, and expand the operational capability to prevent, protect against, respond to, and recover from an incident. It also encompasses effort to recognize and classify potential threats, define vulnerabilities and identify necessary resources for such kind of purposes. Prevention also implicates for suitable measures to protect lives and property. Thus it involves applying intelligence and other data to a variety of actions that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention also contains the stopping of an occurrence before it happens with effective processes, guidelines, standards and certification, following to a proper comprehension of threats together with a suitable vulnerability analysis [18]. Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

As the different sectors that contain CI are very diverse, it would be difficult to prescribe exactly "what criteria should be used to identify and protect all of them" in a horizontal framework; in fact, this has to be carried out on a sector-by-sector basis. Nevertheless, there is a need for a common understanding on certain cross-cutting issues. In the EU it is so proposed that the strengthening of CI can be realized by the setting of a common EPCIP framework (i.e.: common objectives, methodologies e.g. for comparisons, interdependencies [19]) exchanging best practices and compliance monitoring mechanisms.

As all potential critical systems become progressively more complex and are integrated across various geographic and functional borders, relatively small disturbances can rapidly cascade into multifaceted crises. As a result, CI vulnerabilities have garnered high-level political attention in recent years, at the global sector.

The term **"risk analysis"** relates to the consideration of any corresponding threats or of related scenarios, so that to evaluate the vulnerability and the possible influence of disruption or destruction of any corresponding critical infrastructure [20]. There is a considerable number of risk assessment methodologies for CIs. In general, the approach that is used is somewhat common and linear, consisting of several basic components-elements: Identification and classification of threats, identification of vulnerabilities and evaluation of impact. This is a well-known and established approach for assessing risk and it is the backbone of almost all risk assessment methodologies. Nevertheless, there is a vast differentiation of risk assessment methodologies based on the scope of the methodology, the audience to which it is addressed (policy makers, decision makers, research institutes) and their domain of applicability (asset level, infrastructure/system level, system of systems level). These attributes are not mutually exclusive, in the sense that the domain of applicability defines to a certain extent the target group of the methodology [21]. Under this scope, it is suitable and proper to support projects within Member States, to the extent that they can provide useful experience and knowledge for further actions at a broader European level, in particular risk and threat assessments [22].

During the latest years, the appearance of CIP studies and programs at the European level constitutes an increasing trend [23]. Across a number of issue areas, EU Member States have provided substantial initiatives and have selected and promoted appropriate measures for crisis management cooperation [24] through supranational institutions, to ensure a globally accepted character of the proposed measures, as the main target emphasizes upon the protection of people, vital and active systems as well as fundamental societal values from hazardous and risky threats. This sort of dynamic development implicates a qualitatively novel role for the EU, much further beyond pure economic management. In particular, a "European protection policy space" is gradually emerging [25] and is so established. This protection space intersects several policy sectors and EU institutions, thus comprising all activities, mechanisms, resources and other means to deal with potential trans-boundary crises [26].

2. THE INFORMATION TECHNOLOGY (IT) SECTOR AS PART OF THE CI PROTECTION POLICY IN THE MODERN EU CONTEXT

The Information Technology (IT) sector conducts operations and services that provide for the design, development, distribution and support of corresponding products (both hardware/HW and software/SW) and operational support services that are necessary and/or critical to the assurance of national and economic security and public health, safety and confidence. These HW and SW products and services-applications are limited to those essential to maintain or reconstitute the network and its associated facilities or capabilities.

IT sector provides, *among others*, critical control systems and related services/facilities, physical architecture and any relevant Internet infrastructure. Evidently, this sector is fundamental to realize a proper level of the national security, economy, public health and safety. On the other hand, all involved actors (such as corporate entities, authorities, research and academic organizations as well as the public) depend on the proper establishment and the operational functionality of the corresponding resources. Such kind of physical or virtual functions can create and offer hardware, software, and information technology systems and services, under various concepts [27]. Due to the high complexity of the underlying environment which is also under continuous and dynamic evolution, it is usually hard to identify and assess threats or to evaluate and manage vulnerabilities, unless the corresponding effort is performed collaboratively, via the involvement of several appropriate players-entities. The threat analysis context takes into account the broader spectrum of intentional and unintentional manmade and natural threats. As a result of the diverse inherent qualities of manmade deliberate, manmade unintentional, and natural threats, the risk assessment methodology comprises unique, but comparable, components for analyzing these threats and their associated vulnerabilities. The procedure for vulnerability assessment normally considers the people, process, technology, and physical vulnerabilities that, if exploited by a certain kind of threat, could exercise effects and "modify" certain essential features of critical functions (such as confidentiality, integrity, or availability). Although IT technology infrastructure has a convinced level of intrinsic resilience, its interdependent and interconnected structure creates challenges and opportunities for coordinating public and private sector preparedness and protection activities.

The international practice in modern societies and economies implicates that public and private sector partners usually work together to identify principal sector goals that support efforts to prevent, prepare for, protect against, mitigate, respond to, and recover from (nationally) significant events, technological emergencies or disasters that threaten, disrupt, or cripple IT Sector functions. Such goals produce a reciprocally favorable framework to develop risk management and protective strategies, with the aim of enhancing sector security.

IT Sector risk management [28] approaches concentrate on two fundamental levels: (i) The individual enterprise level, and; (ii) the sector -or the national- level. Normally, private sector entities structure their approaches on business explicit objectives, such as shareholder value, efficacy, and customer service. On the other hand, in principle, public sector entities base their approaches on ensuring mission effectiveness or providing a well-defined and conceived public service. Enterprise-level risk management methodologies regularly include cybersecurity initiatives and measures [29] to preserve the well-being of information security programs and of the necessary infrastructures to fulfil that purpose. Corresponding examples may comprise, *inter-alia*: physical vulnerability mitigation measures (e.g., physical access control and surveillance); human vulnerability mitigation measures (e.g., security training and awareness); cybersecurity measures (e.g., encryption; behavior monitoring and management technologies), and; business continuity planning. These individual risk management efforts are considered to support organizational objectives and -in total- they improve the security and resilience of the IT Sector.

The area of ICT security has developed extensively within the EU over the past few years. There is a large body of EU legislation, regulation and programs aimed at the protection of telecommunications, media and IT (the Commission addresses these infrastructures in combination).

Within an area the EU calls "*Network and Information Security (NIS)*", the EU approach includes specific network and information security measures, a regulatory framework for electronic communications (which also addresses issues of privacy and data protection) and measures against cyber crime.

NIS is increasingly significant to our economy and society. NIS is also an important precondition to generate a reliable environment for worldwide trade in services [30]. However, information systems can be affected by security incidents (such as human mistakes, natural events, technical failures or malicious attacks). These incidents are becoming bigger, more frequent, and more complex. Lack of NIS can compromise vital services depending on the integrity of network and information systems. This can harm or terminate businesses functioning, generate substantial financial losses for the economy and negatively affect societal welfare**.** The Member States are responsible for ensuring that the integrity and security of public communications networks are maintained – the level of security or how it should be maintained remains undefined. The current European regulatory framework requires only telecommunication companies to adopt risk management steps and to report serious NIS incidents. However, many other sectors rely on ICT as an enabler and should therefore be concerned about NIS as well. In fact, several infrastructure and service providers are particularly vulnerable, due to their high dependence on appropriately functioning NIS. Such sectors can realize a major role in providing key support services for our economy and society, and the security of their systems is of specific importance to the functioning of the market. (These sectors can include banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, internet services and public administration).

A recent Communication by the European Commission has focused on prevention, preparedness and awareness and defined a plan of immediate actions to strengthen the security and resilience of CIIs [31]. This focus was consistent with the challenges and priorities for NIS policy and the most appropriate instruments needed at EU level to tackle them. The proposed actions were also complementary to those to prevent, fight and prosecute criminal and terrorist activities targeting CIIs and synergetic with current and prospective EU research efforts in the field of NIS, as well as with international initiatives in this area.

The right to privacy and the right to the protection of personal data [32] have been set out in the *Charter of Fundamental Rights*

[33]. During the latest years, in particular, the EU has responded systematically to the challenge posed by the increasing exchange of personal data and the need to ensure the protection of privacy, as it perceives the fact that the technological developments not only present new challenges to the protection of personal data, but also offer new possibilities to better protect it [34]. Elementary principles such as purpose limitation, proportionality, legitimacy of processing, limits on storage time, security and confidentiality as well as respect for the rights of the individual, control by national independent supervisory authorities, and access to effective judicial redress needed to be ensured and a comprehensive protection scheme had to be established.

Within the framework of past European programs as "part" of the *Lisbon Strategy*, the aim was to create common specifications on, for example, personal integrity and user control, and to develop a secure infrastructure. The previously issued *eEurope 2005 Action plan* [35] aimed to improve the robustness of networks and information systems against both accidents and criminal attacks. The European Commission and MS have so worked together with the purpose of developing a secure trans-European communications network through which they could share classified information. The EU has also developed rules to secure electronic communications through such means as measures for electronic signatures and the data protection legislation for electronic communication.

Security of IT networks is one essential factor for a well-functioning information society. This is recognised in the *Digital Agenda for Europe* [36] which addresses issues related to cybercrime, cyber security, safer Internet and privacy as the main components in building trust and security for network users.

The EU has also established a bureau for information security: the *European Network and Information Security Agency* (*ENISA*)[1]. This centre is part of the implementation strategy of the EU ICT policy and is designed to help MS, businesses and industries within the Union to prevent, manage, and solve problems of ICT security. The Member States maintain the overall responsibility for ICT security in their territory. ENISA collects and analyses information from the Member States, using that information to develop recommendations and offer support. Furthermore, the EU has identified that trust and security are fundamental preconditions for the wide uptake of ICT and thus for achieving the objectives of the "smart growth" dimension of the Europe 2020 Strategy [37].

The European Commission has forwarded a *Directive on Network and Information Security* [38] which aimed to strengthen national resilience and to increase cooperation on cyber incidents. This was to be achieved by requiring MS to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures, such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc.), as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

3. CLOUD COMPUTING AS MEANS TO SUPPORT NIS FOR ESSENTIAL CI PROTECTION AND OPERATION

In the previous sections, the importance of network and information systems has been indentified for the majority of all involved CI. Nevertheless, IT Systems used for managing CIs require large resources and hence, CI providers often host their own infrastructure and possess own data centers. However, due to virtually unlimited scalability of resources and performance, as well as noteworthy improvement regarding maintainability, evermore organisations will incorporate cloud computing into their computing environments. Thus, we argue that cloud computing will eventually reach ICT services that are operating critical infrastructures (CI).

Under the term ***cloud computing ("CC")*** we can conceive a "style of computing" where elastic IT-related capabilities are provided as optimized, cost-effective, and on-demand utility-like services to the corresponding customers, mainly by using Internet-based technologies. Cloud computing, in simplified terms, can thus be understood as the storing, processing and use of data on remotely located computers accessed over the Internet. This implicates that "users" can command almost unlimited computing power on demand, that they do not have to make major capital investments to fulfil their needs and that they can get to their data from anywhere, simply with an Internet connection [39].

Being one of the global major trends in the IT industry recently, cloud computing has gained tremendous momentum and started to revolutionize the way enterprises create and deliver IT solutions, via all possible underlying infrastructures. Furthermore, cloud computing has the potential to slash users' IT expenditure and to enable many new services to be developed. As more and more sectors adopt cloud services in their computing environment, the trend also reaches ICT services operating critical infrastructures (CI), such as transportation systems or infrastructure surveillance which are two quite characteristic and modern examples. Cloud services provide competent access to large IT infrastructures that benefit from the economy of scale. In addition, these infrastructures are conceived as "robust enough" due to their replicated and internationally distributed nature. This implicates that it would extremely advantageous to preserve irrecoverable and valuable data obtained from CIs, within secure cloud infrastructures. On the other hand, hosting CI services in the cloud brings with it security and resilience requirements that existing cloud offerings are not "well placed" to deal with, efficiently and satisfactorily, for all related cases. As a result of the complex nature and occasionally dye to the high elasticity of already deployed cloud environments, any attempt to deploy, test and validate CI services in the cloud implicates difficulties and potential obstacles -as well as risks and threats- focused around technical issues but also being dependant upon legal or business issues. Traditional IT security measures cannot fully tackle the issues (e.g. risk, trust, and resilience) arising from this paradigm shift, especially for operators and manufacturers of IT systems for CIs. With a minimum tolerance to any security incidence or downtime, a CI enforces much stronger requirements for security, reliability and resilience on cloud computing environments [40].

As mentioned above, cloud computing offers a host of potential benefits to all involved bodies-entities-actors, including flexibility, scalability, elasticity, high performance, resilience and security, together with cost efficiency [41]. In particular, the cost efficiencies of the cloud stem from aggregating peaks and troughs of demand across a large set of customers. Cloud computing is evolving and includes a wide range of technological solutions and business practices. CC can be assessed with a variety of different meanings in different (complex) contexts. The most widely used definition is the one that has been published by the *US National Institute of Standards and Technology (NIST)* [42] which states

[1] For more information see: https://www.enisa.europa.eu/.

that *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*. The corresponding NIST document defines three basic service models (*SaaS*: Software as a Service; *PaaS*: Platform as a Service, and; *IaaS*: Infrastructure as a Service) and four deployment models (i.e.: public, private, community and hybrid cloud environments). This definition "stresses" the technological configuration of cloud computing, which however may be less important than the changes that it brings. By viewing cloud as a business model the accent can be placed on the key business process characteristics of cloud computing [43] such as: (i) Users do not need to invest in their own infrastructures, storage and processing takes place in the cloud rather than at the users premises or on the user devices; (ii) Cloud services can rapidly scale up or down according to demand; (iii) Cloud virtualises computational power so that the physical location of users or computer resources are no longer a constraint, and; (iv) Computing becomes an operating rather than a capital expenditure item. These are all features that differentiate cloud computing from data centre outsourcing. It gives scale, *or alternatively*, the "illusion of unlimited resources". But it also signals a loss of control as users become reliant upon leased line or public broadband connections and upon the distributed computer systems of the cloud provider. This also distinguishes cloud from grid computing, which does not emphasize this external centralized control but rather the sharing of networked computing resources.

The main concerns about cloud services are security, data location, applicable law and jurisdiction over data, though on the last point it appears that most organizations in the EU market lack a full understanding of the complex issues. Data and application portability between cloud service providers does not appear to be a significant barrier to initial adoption, but becomes more important when the issue is deepening and extending the use of cloud in the enterprise. As, *in principle*, attacks and failures are expected to appear and these cannot be fully eliminated in the cloud environments, it is of critical priority to promote and develop approaches to understanding cloud behaviour in the face of related challenges and attacks [44]. Moreover, for the case where CIs are actually "running" inside the cloud environment, it should be expected that clouds would be a more attractive target for attackers, globally. Thus the countermeasure should implicate for a detailed, in depth, analysis/assessment of all corresponding risks -upon a continuous and fully dynamic perspective- together with preventive -as well as with corrective measures- whenever anomalies, deviations from proper level of operational behaviour or unexpected features may be observed [45].

Due to the great variety of the multiple services that can be offered by the cloud, the latter becomes a quite practical option to include CI in the broader "cloud"-based environment (e.g. resilience to natural disasters, faster recovery in case of failure, etc.); furthermore, this equally creates novel opportunities (i.e., denial of service, service failures, data recovery issues, system attacks, etc.) that may offer benefits to the market. The specific features and the particular attributes of cloud computing implicate that a service structured upon its nature can incorporate a variety of -usually heterogeneous- elements. Any potential combination of these elements -or modules or of all corresponding attributes- may vary over time also depending upon other kinds of influences due to administrative -or other- boundaries. This implicates that any attempt to guarantee security properties of the intended services is difficult, although this may be of significance for CI Systems [46] and thus the handling challenge becomes of greater importance. This is why cloud in the IT industry has put on massive momentum and revolutionised the way enterprises create and deliver IT solutions, also including the CI broader sector.

An interesting option of realizing the above conceptual basis, that for the consideration and use of cloud computing for the support of IT of CI has been recently proposed within the scope of the ***SECCRIT*** *("SEcure Cloud computing for Critical infrastructure IT")* EU-funded project[2]. The *SECCRIT* project's mission is to analyze and evaluate cloud computing technologies with respect to security risks in sensitive environments, and to develop methodologies, technologies, and best practices for creating a secure, trustworthy, and high assurance cloud computing environment for CI. In order to accomplish this mission, the project's objectives have been prescribed as follows: Identification of the relevant legal framework and establishment of respective guidelines, provision of evidence and data protection for cloud services; understanding and managing risk associated with cloud environments; understanding cloud behavior in the face of challenges; establishment of best practice for secure cloud service implementations; and the demonstration of SECCRIT research and development results in real-world application scenarios. An important contribution of SECCRIT was also to provide a sort of reference architecture [47], for suitably supporting the development of technical solution for the provisioning of evidence and data protection for cloud services. An example of the broader intended concept is illustrated in the following *Figure 1*, covering several CI-related potential applications.

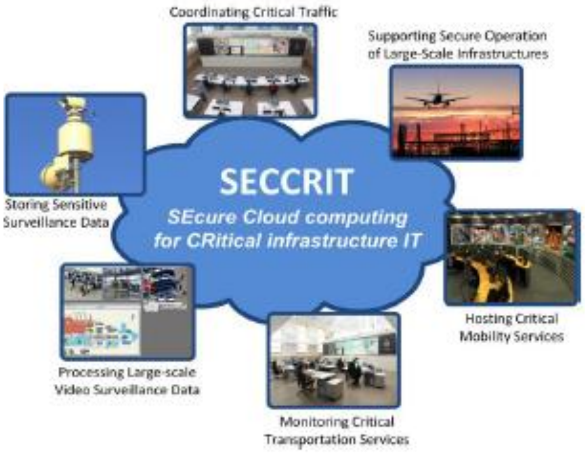
Coordinating Critical Traffic
Supporting Secure Operation of Large-Scale Infrastructures
Storing Sensitive Surveillance Data
SECCRIT
SEcure Cloud computing for CRitical infrastructure IT
Hosting Critical Mobility Services
Processing Large-scale Video Surveillance Data
Monitoring Critical Transportation Services

Figure 1. Scope and potential applications of the SECCRIT-based conceptual framework for CI protection

To reach the above explicitly defined objectives, SECCRIT has promoted a user-driven and multi-disciplinary approach aiming, inter-alia, to the gradual definition of a set of (legal) guidelines about the use of cloud services for CI providers. Furthermore, the project aims upon the development of risk assessment and management methodologies, together with the provision of methodologies and of data as of risk perception, transfer and migration, such that CI providers can make decisions about cloud

[2] More information about the SECCRIT project can be found at: http://www.secrit.eu.

computing adoption with a clear view on the potential risks. To ensure wide adoption and maximise the impact of SECCRIT results, the project solutions should be strongly end user-driven.

4. CONCLUSION

The present work has attempted to identify, discuss and further analyze the concept of critical infrastructures (CIs) and their major importance as “basic tools” for supporting evolution and growth of our modern (Internet-based) societies and economies. Thus, in the first part of our work, we have emphasized upon examining the necessary conceptual terms and the broader framework relevant to the protection and the secure functioning of such infrastructures -and of all related facilities- as parts of modern initiatives and of the actual European strategic framework, *in particular*. We have so focused on particular challenges for an efficient risk management in order to assess, identify and deal with any potential threats and any other sort of harmful events that may affect, disturb, interrupt, cease or even destroy the proper CI operation. Simultaneously, we have discussed, *in detail*, various specific challenges for ensuring a proper level of network and information security and protection within the European territory, in order to properly “reflect” all recently appearing business, social and regulatory challenges, as implicated according to the European policy measures affecting the proper evolution of modern Internet and of any novel infrastructure and of all related sophisticated electronic communications services-facilities. As the challenge of properly managing numerous -and usually heterogeneous- IT resources to serve the above priority becomes a critical factor for success in our modern and complex reality, in particular to serve business-oriented options and corresponding benefits, we have identified the cloud as a “proper means” -or “tool”- to serve that purpose. As an evolutionary development of existing computing and networking technologies, cloud computing has gained tremendous momentum because it establishes a new way to deliver computing and storage resources with flexibility and economies of scale. Thus, it promotes multiple novel concepts and facilities that may revolutionize our technological, business, regulatory and social background; it also implicates for critical challenges that may further affect growth and support the transition towards an globally based information society. Understanding the operational behaviour of cloud services, particularly when challenged, is a paramount concern for CI providers. Root cause analysis techniques that provide insights into the operational behaviour of clouds need to be developed in order to address this important need. This becomes of prime importance as CIs in the cloud are expected to experience numerous malicious attacks while, on the other hand, their operation is to be challenged by faults or (unintended) human mistakes.

As the challenge is quite complex, we provide reference to the actually performed SECCRIT EU-funded research program that intends to develop a resilience management approach that will allow for the use of specific techniques such as diversity and controlled dynamic adaptation of networks and services, in cloud environments.

5. ACKNOWLEDGMENTS

The proposed work has been inspired by the broader concept of the EU FP7 project SECCRIT *(“Secure Cloud computing for Critical infrastructure IT”)* funded by European Commission under the *Grand Agreement No.312758*.

6. REFERENCES

[1] Moteff, J., Copeland, C. and Fischer, J. 2003. *Critical Infrastructures: What Makes an Infrastructure Critical?,* Report for Congress (Library of Congress, Congressional Research Service). Washington, DC. DOI= http://www.fas.org/irp/crs/RL31556.pdf.

[2] Council of the European Union 2008. *Council Directive 2008/114/ EC of 8 December 2008 February 2007 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal (OJ) L345, 75-82.* Council of the European Union, Brussels, Belgium.

[3] Rinaldi S.M, Peerenboom, J.P. and Kelly, T.K. 2001. Identifying, understanding and analysing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21, 6 (December 2001), 11-25. DOI= http://user.it.uu.se/~bc/Art.pdf.

[4] Council of the European Union 2007. *Council Decision of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme “Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks”, Official Journal L58, 1-6.* Council of the European Union, Brussels, Belgium.

[5] Commission of the European Communities 2005. *Green Paper on “A European Programme for Critical Infrastructure Protection” [COM(2005) 576 final, 17.11.2005].* European Commission, Brussels, Belgium.

[6] US President’s Commission on Critical Infrastructure Protection 1997. *Critical Foundations: Protecting America’s Infrastructures*. Washington, DC. DOI= https://fas.org/sgp/library/pccip.pdf.

[7] Yusta, J.M., Correa, G.J. and Lacal-Arántegui, R. 2011. Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy* 39, 10 (October 2011), 6100-6119.

[8] Metzger, J. 2004. The concept of critical infrastructure protection. In *Business and Security Public-Private Sector Relationships in a New Security Environment*, Bailes, A. and Frommelt, I. (Eds). Oxford University Press, New York, NY 197-209.

[9] Sterbenz, J.P.G., Hutchison, D., Çetinkaya, E.K., Jabbar, A., Rohrer, J.P., Schoeler. M. and Smith. P. 2010. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54, 8 (June 2010), 1245-1265.

[10] European Council 2010. *Conclusions of the European Council of 10/11 December 2009 on “The Stockholm Programme”- An Open and Secure Europe serving and protecting citizens (2010-2014), Official Journal C115, 04.05.2010, 1-38.* European Council, Brussels, Belgium.

[11] Commission of the European Communities 2010. *The EU Internal Security Strategy in Action: Five steps toward a more secure Europe [COM (2010) 673 final, 22.11.2010].* European Commission, Brussels, Belgium.

[12] Commission of the European Communities 2014. *The Final Implementation report on the EU Internal Security Strategy 2010-2014 [COM (2014) 365 final, 20.06.2014].* European Commission, Brussels, Belgium.

[13] Krger, W. 2008. Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety*, 93, 12 (December 2008), 1781-1787.

[14] Lewis, A.M., Ward, D., Cyra, L. and Kourti, N. 2013. European reference network for critical infrastructure protection. *International. Journal of Critical Infrastructure Protection*, 6, 1 (March 2013), 51-60.

[15] Commission of the European Communities 2012. *Commission Staff Working Document on the Review of the European Program for Critical Infrastructure Protection (EPCIP) [SWD(2012) 190 final, 22.06.2012]*. European Commission, Brussels, Belgium.

[16] Commission of the European Communities 2004. *Communication on Critical Infrastructure Protection in the fight against Terrorism [COM(2004) 702 final, 20.12.2004]*. European Commission, Brussels, Belgium.

[17] Commission of the European Communities 2006. *Communication on A European Programme for Critical Infrastructure Protection [COM(2006) 786 final, 12.12.2006]*. European Commission, Brussels, Belgium.

[18] Sarewitz, D., Pielke, R. and Keykhah, M. 2003. Vulnerability and risk: Some thoughts from a political and policy perspective. *Risk Analysis*, 23, 4 (April 2003), 805-810. DOI= http://sciencepolicy.colorado.edu/admin/publication_files/2003.23.pdf.

[19] Rosato, V. 2008. Modelling interdependent infrastructures using interacting dynamic models. *Int. J. Critical Infrastructures*, 4(1/2), 63-79. DOI= 10.1504/IJCIS.2008.016092.

[20] Bier, V.M. 2009. Game *Theoretic Risk Analysis of Security Threats*. Springer, New-York, NY.

[21] Giannopoulos, G., Filippini, R. and Schimmer, M. 2012. *Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art - JRC Technical Notes*. European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, Luxembourg.

[22] Lindberg, A.-K., Hansson, S.O. and Rollenhagen, C. 2010. Learning from accidents - What more do we need to know?, *Safety Science* 48, 6 (July 2010), 714-721.

[23] Burgess, J.P. 2007. Social values and material threat: the European Programme for Critical Infrastructure Protection. *Int. J. of Critical Infrastructures*, 3(3/4), 471-487. DOI= 10.1504/IJCIS.2007.014121.

[24] Hart, P. 't, Heyse, L. and Boin, A. 2001. Guest Editorial Introduction. New trends in crisis management. Practice and crisis management research: Setting the agenda. *Journal of Contingencies and Crisis Management* 9, 4 (December 2001), 181-188. DOI= 10.1111/1468-5973.00168.

[25] Boin, A., Ekengren, M. and Rhinard, M. 2006. Protecting the Union: Analyzing an emerging policy space. *Journal of European Integration*, 28, 5 (November 2006), 405-421.DOI= 10.1080/07036330600979573.

[26] Rosenthal, U., Boin, R.A. and Comfort, L.K. 2001. *Managing Crises: Threats, Dilemmas, Opportunities*. Charles C. Thomas, Springfield, IL.

[27] US Department of Homeland Security 2010. *Information Technology Sector-Specific Plan - An Annex to the National Infrastructure Protection Plan*. Washington, DC. DOI= http://www.it-scc.org/uploads/4/7/2/3/47232717/nipp-ssp-information-tech-2010.pdf.

[28] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 2011. *Information technology - Security techniques - Information security risk management, ISO/IEC 27005:2011*. ISO, Geneva, Switzerland.

[29] US Department of Homeland Security 2010b. *Enabling Distributed Security in Cyberspace Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*. Washington, DC, 2010. DOI= http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

[30] Commission of the European Communities 2006b. *Communication on A strategy for a Secure Information Society – "Dialogue, Partnership and Empowerment" [COM(2006) 251 final, 31.05.2006]*. European Commission, Brussels, Belgium.

[31] Commission of the European Communities 2009. *Communication on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" [COM(2009) 149 final, 30.03.2009]*. European Commission, Brussels, Belgium.

[32] European Parliament and Council 2002. *Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L201, 31.07.2002, 37-47*. European Parliament and Council, Brussels, Belgium.

[33] European Communities 2000. *Charter of the Fundamental Rights of the European Union, OJ C364, 18.12.2000, 1-22*. European Communities, Brussels, Belgium.

[34] Commission of the European Communities 2012b. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General data Protection Regulation) [COM(2012) 11 final, 30.03.2012]*. European Commission, Brussels, Belgium.

[35] Commission of the European Communities 2002. *Communication on eEurope 2005: An Information society for All [COM(2002) 263 final, 28.05.2002]*. European Commission, Brussels, Belgium.

[36] Commission of the European Communities 2010b. *Communication on A Digital Agenda for Europe [COM(2010) 245 final, 19.05.2010]*. European Commission, Brussels, Belgium.

[37] Commission of the European Communities 2010c. *Communication on Europe 2020 - A Strategy for Smart, Sustainable and Inclusive Growth [COM(2010) 2020 final, 03.03.2010]*. European Commission, Brussels, Belgium.

[38] Commission of the European Communities 2013. *Proposal for a Directive of the European Parliament and of the concerning measures to ensure a high common level of network and information security across the Union [COM(2013) 48 final, 07.02.2013]*. European Commission, Brussels, Belgium.

[39] Commission of the European Communities 2012c. *Communication on Unleashing the Potential of Cloud Computing in Europe [COM(2012) 529 final, 27.09.2012*]. European Commission, Brussels, Belgium.

[40] Takabi, H., Joshi, J.B.D. and Ahn, G.-J. 2010. Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, 8, 6 (November/December 2010), 24-31. DOI= http://doi.ieeecomputersociety.org/10.1109/ MSP. 2010.186.

[41] Catteddu, D. 2011. *Security and Resilience in Governmental Clouds. Making an informed decision*. European Network and Information Security Agency (ENISA). DOI= http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds.

[42] Mell, P. and Grance, T. 2011. *The NIST Definition of Cloud Computing. NIST Special Publication 800-145*. National Institute of Standards and Technology (NIST), Gaithersburg, MD. DOI= http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[43] Kushida, K.E., Murray, J. and Zysman, J. 2012. The gathering storm: Analyzing the cloud computing ecosystem and implications for public policy. *Communications and Strategies*, 85, 1st quarter 2012, 63-85.

[44] Cloud Security Alliance (CSA) 2011. *Quick Guide to the Reference Architecture - Trusted Cloud Initiative*. Cloud Security Alliance. DOI= https://cloudsecurityalliance.org/ media/news/csa-announces-tci-white-paper/.

[45] de Bruijne, M. and van Eeten, M. 2007. Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. *Journal of Contingencies and Crisis Management*, 15, 1 (February 2007), 18-29. DOI= 10.1111/j.1468-5973.2007.00501.

[46] Hudic, A., Hecht, T., Tauber, M., Mauthe, A. and Cáceres, S.E. 2014. Towards continuous cloud service assurance for critical infrastructure IT. In *Proceedings of the IEEE 2014 International Conference on Future Internet of Things and Cloud* (Barcelona, Spain, August 27-29, 2014. FiCloud, IEEE Computer Society, Washington, DC, 175-182. DOI= 10.1109/FiCloud.2014.36.

[47] Bless, R., Schöller, M., Smith, P., Pallas, F. and Horneber, J. 2013. An architectural model for deploying critical infrastructure services in the cloud. In *Proceedings of the IEEE International Conference on Cloud Computing Technology and Science 2013* (Bristol, UK, December 02-05, 2013). IEEE CloudCom 2013, IEEE, Washington, DC, 458-466. DOI= 10.1109/CloudCom.2013.53.