Critical Infrastructure Protection: A Holistic Methodology for Greece

Dimitris Gritzalis[1(✉)], George Stergiopoulos[1], Panayiotis Kotzanikolaou[2], Emmanouil Magkos[3], and Georgia Lykou[1]

[1] Information Security and Critical Infrastructure Protection Laboratory, Department of Informatics, Athens University of Economics and Business, 76 Patission Avenue, 10434 Athens, Greece
{dgrit, geostergiop, lykoug}@aueb.gr
[2] Department of Informatics, University of Piraeus, 85 Karaoli & Dimitriou Street, 18534 Piraeus, Greece
pkotzani@unipi.gr
[3] Department of Informatics, Ionian University, 7 Tsirigoti Square, 49100 Corfu, Greece
emagos@ionio.gr

Abstract. The protection of Critical Infrastructures (CI) is, by definition, of high importance for the welfare of citizens, due to direct threats (dictated by the current international political situation) and also due to their dependencies at international and European levels. Today, Greece remains one of the countries of the European Union, which has no comprehensive strategy to safeguard national CI, nor any process of developing such an integrated plan, except for some initiatives taken from the General Secretariat of Digital Policy. This paper aims to contribute to: (i) The creation of an inventory of all stakeholders, (legislative, supervisory or regulatory) involved in CI protection in Greece, (ii) the identification of potential national CI, as well as their interdependencies, (iii) the development of a structured identification based on impact assessment methodology for national CI, that takes into account internationally applied CI assessment methodologies, and (iv) provide a pilot implementation of the proposed methodology.

1 Introduction

The protection of Critical Infrastructures (CI) is, by definition, of high importance for the welfare of citizens of each country; especially nowadays, both because of direct threats (dictated by the current international political situation) and also due to emerging interactions or dependencies [13–15] developed between national CI at international and European levels.

Today, Greece remains one of the few countries of the European Union, which, be-sides the formal transposition of the 114/2008/EC Directive into domestic legislation, has not implemented a comprehensive CI protection strategy, nor any process of developing such an integrated plan, except for some initiatives taken by the General Secretariat of Digital Policy.

N. Cuppens-Boulahia et al. (Eds.): CyberICPS 2016, LNCS 10166, pp. 19–34, 2017.
DOI: 10.1007/978-3-319-61437-3_2

This paper presents some of the results which derived from project OLIKY[1] that aimed to provide a road-map towards the development of a holistic national CIP strategy for Greece. The basic goals of OLIKY included, among others:

1. The initial creation of an inventory and an initial ranking of candidate national CI, along with their supervised entities, in order to identify the most critical services and their dependencies, to adequately protect and increase their resilience against known or unknown threats.
2. The assessment of critical services and interdependencies between candidate national CI based on a methodology for the classification of national critical components.

The objectives of the OLIKY project did not include a comprehensive coverage and assessment of all national CI, nor the proposal of a detailed security policy for each CI. This would not be feasible in the context of an independent study, since the complete recording and evaluation of all CI nationwide requires an authorized body with the institutional and legal feasibility of collecting and processing classified information along with the cooperation of all national CI operators. However, an initial systematic identification and evaluation of Greek CI may act as a catalyst for conducting such an in-depth analysis.

Contribution. The main contributions of this paper include:

1. The development of an inventory of all stakeholders, (legislative, supervisory or regulatory) involved in the protection of the Greek CI.
2. The identification of potential national CI, as well as their interdependencies. In particular, an attempt was made to identify national CIs on the Energy, Transport and Information and Communication Technologies (ICT) sectors.
3. The development of a structured identification methodology for national CI, taking into account internationally applied CI identification methodologies. A range of three evaluation levels (criticality) and specific evaluation criteria for the integration of critical components in criticality levels will also be developed and utilized, as part of the proposed methodology.
4. The pilot implementation of the proposed methodology to a list of candidate national CI fields in order to rank their criticality; namely on the Energy and ICT sectors.

2 A Preliminary Record of Greek Critical Infrastructures

The identification and evaluation of national CI first requires the creation of an initial list of potential CI, at sector and subsector levels. In this section, the services of three key critical sectors of the country are being mapped; namely those concerning the Energy, Transport and ICT sectors.

[1] All OLIKY project deliverables (in Greek) can be found at: http://www.dianeosis.org/2016/07/ideas_infrastractures_protection/.

As part of a national CI protection program, each EU Member-State (MS) is re-quired to: (i) record its National Critical Areas, (ii) record and evaluate the systems or parts thereof which may constitute a CI, and (iii) to record and evaluate (possible) inter-dependencies between the identified CI. Also, each MS has to plan and/or up-date a Business Continuity Plan (BCP) and a Contingency Plan (CP) for the protection of its national CI [1–6]. Since, in most cases, the owners and/or operators of CI are private entities, any national CI identification process (along with all processes in the context of a national protection program) requires the exchange of information between stakeholders, in accordance with the principle of collaboration between stakeholders and the Public-Private Partnership (PPP) [12]. During the stage of critical area identification, each MS must establish an initial list of critical national sectors, i.e. sectors existing in the geographical limits of the country that include contingent CI. Still, the process of selecting national critical sectors and sub-sectors is not obvious [2].

Towards creating a common framework program for the EPCIP (European Programme for Critical Infrastructure Protection) the establishment of a common list of critical sectors/subsectors is highly encouraged [1–6]. The concept of critical service is often used by implication instead of the term infrastructure, since it integrates the existence of a set of goods and processes that need protection and are examined in general and with detailed analysis. The list of CI is presented in Table 1 and incorporates the concept of service per subsector.

Table 1. List of potential CI, sectors, and subsectors selected for Greece

Sector	Subsector	Service
Energy	Electricity	Generation (all forms)/ Transmission
		Distribution/Electricity market
	Oil	Extraction/Refinemen
		Transport/Storage
	Natural gas	Extraction/Transport
		Distribution/Storage
Information and communication technologies (ICT)	Information technologies	Web services/Internet
		Computer networks/Services cloud
		Software as a service (SaaS)
	Communications	Voice/Data communications
		Mobile communications/Satelite
		Radio communication/Broadcasting
Water	Drinking water	Water storage/Quality assurance
		Water distribution
	Wastewater	Wastewater collection & treatment

(*continued*)

Table 1. (*continued*)

Sector	Subsector	Service
Food	Food supply chains	Agriculture/Food production
		Food supply
		Food distribution/Quality/Safety
Health	Hospital & heath facilities	Emergency healthcare/Hospital care (inpatient & outpatient)
		Supply of medicines, vaccines, blood & medical supplies
		Control of infections and epidemics
Financial services		Banking/Stock exchange
		Payment transactions
Public order & security	Public order	Maintenance of public order and safety
	Justice	Judiciary and penal systems
Transportations	Aviation	Air navigation services
		Airport operation
	Road transport	Bus/Tram services/Road network maintenance
	Train transport	Railway network management
		Railway transport services
	Maritime transport	Navigation control - cruises
		Coastal interconnection
	Postal services	Logistic services
		Payment transactions
Industry	Critical industries	Employment/GDP/Supply of goods
	Chemical/Nuclear industry	Storage & disposal of hazardous materials
		Safety of high risk industrial units
	Tourism	Hotel supplies
		Restaurant supplies
	Agriculture	Agricultural unit supply
		Water supply services
Public administration	Government/Ministries	Government functions
	Regional administration	Civil services
Civil protection		Emergency and rescue services

(*continued*)

Table 1. (*continued*)

Sector	Subsector	Service
Environment		Air pollution monitoring and early warning
		Meteorological monitoring and early warning
		Ground water (lake/river) monitoring and early warning
		Marine pollution monitoring and control
Defense		National defense

In order to identify candidate Greek CI, the ENISA List of Critical Sectors and Related Critical Services [7] was used to create an overview of the Critical Sectors as reported in Table 1, where specific areas were selected as being more significant for the country. Potential critical services which were irrelevant to Greek Activities (e.g. Space sector) were removed from the list due to non-conformity, while others have been added due to their potentially high impact on Greece's GDP, like Tourism and associated services.

Based on the collection of public information and scientific expertise of the panel members, the following critical areas were selected for our study: (a) Energy (b) Information and Communications Technologies (ICT) and (c) Transportation.

Results from identifying interdependencies and main stakeholders for these three fundamental CI sectors are presented in Tables 2, 3 and 4, respectively. These tables contain critical domains, sub domains for each critical service, the key subsystems that are necessary for providing each service, the essential interdependencies with other (sub) sectors, as well as an inventory of the providers of each service involved in the country.

Energy sector

In Greece, multiple providers support various subsectors of the Energy sector. In some subsectors, only one provider (or a very small number of them) has a dominant position, making him the obvious choice for a CI at the Energy sector. Still, some changes have occurred in the Energy market of other subsectors over the last years; usually because of Greece's need to comply with the relevant European Directives, but also due to the economic situation of the country.

ICT sector

The Information and Telecommunication Technologies (ICT sector) is a sector of high criticality since it provides information assets and services to almost all other critical services in the country. Of all the ICT subsectors, it appears that the Telecommunication subsector is the most important in Greece. Hardcore centralization of services is observed at the Greek ICT sector, although for some services there seems to be a more balanced distribution of providers. For this reason several providers have been identified as candidate CI for this sector although their "weight" may significantly vary.

Table 2. Summary of the energy sector in Greece

Critical subsector	Critical service	Interdependencies		Main Stakeholders
		Depends upon	Affects	
Electricity	AC/DC production	Mining of lignite	All sectors	Public power corporation
		General transfer		Alternative electric power producers
		Oil transfer		PPC Renewables
	Transportation/Storage	All sectors	All sectors	Hellenic electricity distribution network operator
	Electrical. Energy market	Production	All sectors	Public power corporation
		Distribution		Alternative electric power producers
Oil	Mining	Refinement	Industry	Energean oil & gas
		Transport		
		Storage		
	Refinement	Transport storage	Business	Hellenic Petroleum
				Motor Oil Hellas
	Transport	Shipping	Agriculture	Hellenic Petroleum
		Internal relations	Transportation	Shipping Sector
	Storage	Oil transfer		Motor Oil Hellas
				Hellenic Petroleum
Natural Gas	Transportation/Distribution	Cross-border	Industry Domestic use	Public Gas Corp. TAP (under construction)
		Interconnections		
		External relations		
	Storage	Transport/Distribution		Puplic Gas Corp.
		External relations		(LNG Revithousa)

Table 3. Summary of the ICT sector in Greece

Critical Subsector	Critical Service	Interdependencies		Main Stakeholders
		Depends upon	Affects	
Telecoms	Voice/Data coms	Power supply internet access external links	All sectors	OTE Group (COSMOTE, OTEGlobe, OTESAT - MARITEL, CosmoOne) Vodafone Greece WIND Hellas Forthnet CYTA
	Internet access	Voice/Data		
		Communications		
		External Links		
Information technologies	Data centers/Cloud services	Power supply	Economy Business Industry	Med nautilus OTE Lamda Helix
		Providing		
		Telecommunications		
		Internet access		
		Tel/Stances (ext. links)		
	Web services	Power Supply providing telecoms Internet access ICT ConAbroad	Economy business	Telecommunications providers small providers

Table 4. Summary of the transportation sector in greece

Critical Subsector	Critical Service	Interdependencies		Main Stakeholders
		Depends upon	Affects	
Road transport	Motorways, national and provincial roads	Availability of oil	Provision of road transportation	Min. of infrastructure and transport technical contractors (Companies)
		ICT Systems		
		Interoperability infrastructure	Social & economic growth	
		Environment & weather		
	Provision of road passenger transport and cargo	Motorways, national and provincial Roads	Trade	National and international transport companies
		Availability of oil	Government	Transport agencies
		Road Signage	Business	Urban Transport: OASA, OSY, STASY
		Environment & weather	Industry	OASTH
			Agriculture	Suburban buses

(*continued*)

Table 4. (*continued*)

Critical Subsector	Critical Service	Interdependencies		Main Stakeholders
		Depends upon	Affects	
Shipping	Ports and port infrastructure	Availability	Providing ferry transport	Min. of infrastructure and transport
		ICT Systems	Trade	Min. of Shipping and Island Policy
		Interoperability infrastructure	Industry	Piraeus Port Authority SA COSCO SA
		Environment & weather	Enterprises	Thessaloniki port authority SA
			Agriculture	Greek port authorities
	Coastal transport & transportation	Port infrastructure	Tourism	Ferry operators transport companies Tourist companies
		Availability of mineral resources & energy	Trade	
		Marine signaling system	Industry	
		ICT systems	Enterprises	
		Environment & weather	Agriculture	
Aviation	Airports and airport infrastructure	Availability	Air transportation tourism	Hellenic civil aviation authority
		ICT systems		Athens international airport
		Interoperability infrastructure		Hellenic republic asset development fund
		Environment & weather		
	Air transport	Availability petroleum	Tourism Trade	Hellenic civil aviation authority AIRCARRIERS
		System radar air navigation services		
		ICT Systems	Government agencies	EUROCONTROL
		Environment & Weather		
Rail Transport	Network Rail infrastructure	Communications systems & information	Trade industry	Greek Railways/OSE SA
				ERGOSE SA
				GAIAOSE SA

(*continued*)

Table 4. (*continued*)

Critical Subsector	Critical Service	Interdependencies		Main Stakeholders
		Depends upon	Affects	
	Rail transport	Rail infrastructure network	Trade	Greek railways companies
		Energy availability	Industry	TRAINOSE SA
		ICT systems	Business	STASY SA
		Interoperability infrastructure	Agriculture	AMEL SA
			Tourism	TRAM SA

Transportation Sector

The transport sector provides services to multiple other sectors and supports many economic activities such as trading, tourism, industry, rural development and the exploitation of natural resources of Greece. The sector is subdivided into Road, Sea, Air and Rail transport along with postal services.

3 Method for Determining and Evaluating National CI

This section describes a methodology for identifying and evaluating national CI, structured as a sequence of steps. Each step provides a brief description, the data (or parameters) input necessary for the execution, and implementation actions needed and expected results. The development of the methodology took into consideration previous work from other EU members [7–12, 16–20, 26], since following a best practice and creating a common baseline throughout the EU is of outmost importance.

Categories of criteria for the integration of candidate CI were defined inside the methodology. These include direct assessment criteria, time-based criteria and indirect criteria used to evaluate the "importance" of the CI. Direct evaluation criteria are based on the assessment of potential impact (impact-based classification) that are expected to manifest after an attack on relevant infrastructures.

Time-based criteria such as estimated recovery time, and estimated impact evolution over time are used for prioritizing CI within each risk level. Indirect criteria consider, amongst others, second order dependencies, which may eventually upgrade a candidate CI to a higher criticality level, e.g., when other critical elements depend on it. Indeed, the analysis of interdependencies between CI can identify CI that might have been underestimated during previous analysis [13–15, 21–25].

For each critical service sectorial and horizontal criteria are utilized for the identification of its most important subsystems. The methodology does not take into account threats (threats or scenarios), nor does it assess them according to their likelihood. A schematic overview of the described Methodology is presented in Fig. 1.

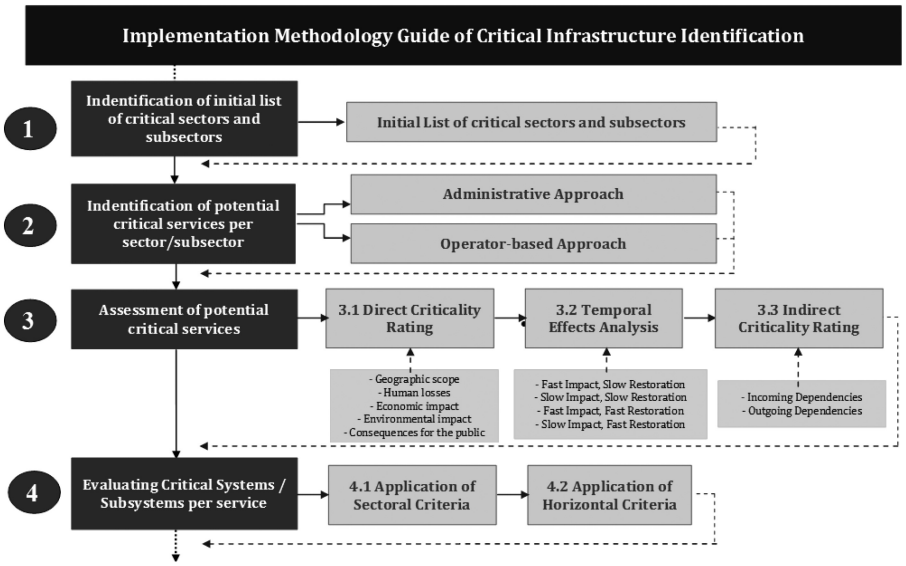

Fig. 1. Schematic overview of the methodology

STEP 1: Initial list of critical sectors and subsectors

Short description. In the first step an initial list of potential national critical sectors and subsectors per sector is catalogued. Sectors and subsectors from the list of services offered in Table 1 are used as input.

Implementation. Cataloguing of the initial sectors/-subsectors list is performed by a central authority. Typically, this can be coordinated by the respective competent body for the protection of national CI.

Results. The initial list of critical sectors/sub-sectors will be given as input to Step 2 and Step 3.

STEP 2: Identify potential critical services per sector/subsector

Short description. For each critical area, potential critical services are identified. The list compiled from Step 1 can be considered as initial parameter in the process of identifying potential critical services per sector/sub-sector, along with good-practices from EU members [9–12] which are mature enough when it comes to implementing strategies for the protection of national CI.

Implementation. There are two alternative approaches that can be followed to identify possible national critical services sector/subsector [7]:

Administrative Approach. A list of potential national critical sector services is compiled at a central, administrative level, in cooperation with a competent Authority. According to Operator-based approach, a Critical Operator list is compiled (in-line with relevant legal frameworks). Operators will be responsible to identify critical services that are involved in.

Results. The list of critical services sector/subsector will be given as input to Step 3 for the risk assessment of possible critical services per sub-sector.

STEP 3: Assessment of potential critical services

Short description. Possible critical elements from previous steps (sub-sector and/or services by sub-sector) are assessed and prioritized using specific criteria. Initial parameters that can be considered for the evaluation of potential critical subsectors/services are:

- The initial list of possible critical sectors/subsectors from Step 1.
- The initial list of potential critical services from Step 2 (this list may include the list from Step 1).
- The non-binding guidelines of the European Council [5] on the implementation of the horizontal criteria during the evaluation of CI.
- Good practices from EU members [12].

Implementation. Depending on the approach taken during Step 2 (Administrative approach or Operator-based approach), the following checks are applied, either at central level or in collaboration with Critical Administrators:

*Step 3.*1. *Direct criticality rating*. All potential critical services are assessed, based on the immediate consequences that would result from their breach or failure. This is achieved by applying selected horizontal criteria, from the following list [5, 6]:

- Geographic scope: The scope of the area to be affected by an event.
- Human losses: The number of victims and/or injured people.
- Economic impact: The impact in a macro and/or macro-social level.
- Environmental impact: Long-term environmental effects.
- Consequences for the public: Impact of events affecting the people, which does not directly relate to any of the previous criteria.

*Step 3.*2. *Temporal effects analysis*. The following are evaluated for each critical service: (a) the time required for the manifestation of maximum impact and (b) the time required to fully restore a service after a possible attack manifestation. Time analysis is used for the classification of critical services within each level of criticality. Temporal analysis is used for prioritizing services within the same criticality level. Specifically, depending on the scores for (a) and (b) each critical element is assigned to a specific category (Step 3.3).

*Step 3.*3. *Indirect criticality rating*. Any possible critical service is also analyzed based on the indirect effects that can cause during a failure scenario. Indirect effects depend on two factors:

- Dependencies of the service in question with other critical services. Whether and how much other critical elements may depend on this particular service.
- Evaluation of indirect criticality is performed by utilizing one or more horizontal criteria, from Step 3.1.

Results. The list of prioritized sub-sectors and services per sub-sector, as well as a table of interdependencies between sub-sectors/services will be provided as input to Step 4, to assess the criticality of (sub) systems per critical service. This step determines a list of possible European critical sectors/subsectors or services. For each horizontal criterion to be applied, criticality levels are described using a quality scale (e.g. Low, Medium, High). For each level, a minimum quantitative impact threshold is set.

STEP 4: Evaluating Critical (sub) systems per service
Short description. For each critical service, a list of involved owners-managers is compiled, from which (or in collaboration with whom) a second list of the most critical subsystems that support this service is compiled.

Implementation. According to the approach proposed by the EPCIP framework [5, 6], certain criteria must be applied at each sub-sector for the characterization of a subsystem as a possible CI inside a service (Step 4.1). This is to check whether a subsystem meets at least one horizontal criticality criterion (Step 4.2).

Results. This step provides a list of the most critical subsystems per service. This will be the actual list of national CI, according to the 114/2008/EC Directive. As part of a National CI Protection Program, CI owners-operators in collaboration with a qualified national body must identify the most important assets per critical subsystem and develop Operation Security Plans (OSP) and Contingency Plans (CP) to protect the CI (Annex II - 114/2008/EC Directive).

*Step 4.*1: *Application of Sectoral Criteria*: Sectoral criteria are technical or operational criteria used to identify potential critical subsystems. These criteria do not report, although hint, potential repercussions (e.g. obstruction or shutdown of a subsystem). Instead, they only refer to certain inherent characteristics. In particular, the sectoral criteria may refer to [5, 6]:

- Technical properties. For example, quantifiable characteristics, such as dimensions, capacities, distances, speed, data volume, etc.
- Non-technical properties. For example, identifiable features such as recovery time, recovery costs etc.

To identify a subsystem as potentially critical, it should exceed a predetermined threshold (threshold) concerning the values of some sectoral criteria.

*Step 4.*2: *Application of Horizontal Criteria*: For each subsystem that provides essential services, we assess the severity that its loss or dysfunction would have on society. A subsystem is critical when it meets at least one of the horizontal criticality criteria, concerning the direct (Step 3.1) or indirect criticality (Step 3.2). Also, criticality evaluation takes into account parameters such as the availability of alternatives, the turning-point for "painful" consequences, as well as the time needed for recovery.

STEP 5: Periodic re-assessment of CI
Short description. All critical and relevant factors concerning the criticality of a CI and relevant services should be reassessed after some time by applying all steps of the methodology at regular intervals.

Input data. All results of the previous evaluation of critical components (sectors, sub-sectors, services, systems).

Implementation. The reassessment may be general (step 1, taking into account the previous critical services list), or may refer to a particular sector/subsector (step 3) or service (step 4). The reassessment scope is determined by a qualified body in collaboration with stakeholders. The need for reassessment should be determined on a mid-term basis; the period must be fixed in advance, regardless of whether changes in the collected data occur or not.

Results. The amended list of critical elements and CI or the update of the previous assessment of critical components (domains, subdomains, services and systems.

3.1 Applying Evaluation Criteria on Candidate National CI

After establishing all parameters for evaluating potential CI, the description of the national CI assessment methodology is complete and will now be applied to the Greek Energy and ICT sectors. During the implementation of the horizontal evaluation criteria, the estimated impact always refers to the worst-case scenario.

Therefore, when analyzing potential impact values listed in the tables below, the value attributed to each impact corresponds to the most negative potential effect that is likely to occur.

Also when we applied the criteria, there happened to be some cases where the assessment could not get unique value assignments, thus values were assigned on the 1–2 impact scale. When a qualified national body implements a full version of the above methodology, every service criterion should be assigned only one scale value.

Energy Sector evaluation

The Energy Sector includes the following sub-sectors: Electricity, Oil and Natural Gas. Tables 5, 6 and 7 summarize the evaluation of each sub-sector and key dependencies recorded, incoming and outgoing, by sub-sector.

Table 5. Application of Criteria - Electricity subsector

Services	Direct assessment (Horizontal Criteria)					Time criteria		Indirect assessment (due to dependencies)
	Geographic al width	Economic Loss	Human casualties	Environmental Cons.	Consequences to the Public	Time of consequence manifestation	Recovery Time	
Production of electrical power	Territory	Important % of GNP	Potential Loss in case of accident	Potential in case of accident	Effect on the lives of million citizens	Rapid consequence manifestation Slow recovery		Affects most CIs
	LEVEL 3	LEVEL 3	LEVEL 1	LEVEL 1	LEVEL 3	CATEGORY 3		LEVEL 3
Transportation/Distribution of electrical power	Territory	Important % of GNP	Potential Loss due to impact on Health Sector		Effect on the lives of million citizens	Rapid consequence manifestation Slow recovery		Affects most CIs
	LEVEL 3	LEVEL 3	LEVEL 1		LEVEL 3	CATEGORY 3		LEVEL 3
Electrical power market	Territory	Important % of GNP			Effect on the lives of million citizens	Rapid consequence manifestation Slow recovery		Affects most CIs
	LEVEL 3	LEVEL 3			LEVEL 3	CATEGORY 2		LEVEL 3

Based on the application of the evaluation criteria and taking into account the record from providers/-operators per service, our evaluation provided the following:

- In the Electricity sub-sector all services are assessed as high critical, both for direct and indirect dependencies. To an extent, they also depend on one provider/IM (PPC).
- Concerning the temporal analysis of impact, the Production and Distribution services have higher priority than the electricity market service, as far as recovery time is concerned.
- At the subsystems level, all subsystems used to support this sector's services must be tested using corresponding sectoral criteria.

Table 6. Application of criteria - oil subsector

Services	Direct Assessment (Horizontal Criteria)					Time criteria		Indirect assessment (due to dependencies)
	Geographical width	Economic loss	Human casualties	Environmental Cons.	Consequences to the Public	Time of consequence manifestation	Recovery Time	
Oil extraction			May cause loss of life	Serious consequences				
			LEVEL 1	LEVEL 1 or LEVEL 2				
Oil refinement	Territory	Important % of GNP	May cause loss of life	Serious consequences	Effect on the lives of million citizens	Slow consequence manifestation Slow recovery		Affects most CIs
	LEVEL 3	LEVEL 3	LEVEL 1	LEVEL 1 or LEVEL 2	LEVEL 3	CATEGORY 2		LEVEL 3
Oil transportation	Territory	Important % of GNP	May cause loss of life	Serious consequences	Effect on the lives of million citizens	Slow consequence manifestation Slow recovery		Affects most CIs
	LEVEL 3	LEVEL 3	LEVEL 1	LEVEL 1 or LEVEL 2	LEVEL 3	CATEGORY 2		LEVEL 3
Oil storage	Territory	Important % of GNP	May cause loss of life	Serious consequences	Effect on the lives of million citizens	Slow consequence manifestation Slow recovery		Affects most CIs
	LEVEL 3	LEVEL 3	LEVEL 1 or LEVEL 2	LEVEL 1 or LEVEL 2	LEVEL 3	CATEGORY 2		LEVEL 3

Table 7. Application of criteria - natural gas subsector

Services	Direct Assessment (Horizontal Criteria)					Time Criteria		Indirect Assessment (due to dependencies)
	Geographical width	Economic Loss	Human Casualties	Environmental Cons.	Consequences to the Public	Time of consequence manifestation	Recovery Time	
Transportation & distribution of natural gas	Territory	Important % of GNP	Potential loss in case of accident	Low consequences	Effect on the lives of million citizens	Rapid consequence manifestation Slow recovery		Affects > 2 CIs (Industry, Electricity Production)
	LEVEL 3	LEVEL 3 or LEVEL 2	LEVEL 1 or LEVEL 2	LEVEL 1 or LEVEL 0	LEVEL 3	CATEGORY 3		LEVEL 3
Natural Gas storage	Territory	Important % of GNP	Potential loss due to impact on health sector	Low consequences	Effect on the lives of million citizens	Rapid consequence manifestation Slow recovery		Affects > 2 CIs (Industry, Electricity Production)
	LEVEL 3	LEVEL 3/LEVEL 2	LEVEL 1/LEVEL 2	LEVEL 1/LEVEL 0	LEVEL 3	CATEGORY 2		LEVEL 3

ICT Sector evaluation

The ICT sector includes the Telecommunications and Information Technologies subsectors. Table 8 presents the evaluation of these subsectors.

Based on the application of the evaluation criteria and taking into account the record from providers/operators per service, our evaluation provided the following:

- The Communications sub-sector has increased impact in Greece. All services showed that they are of high criticality, both in direct and in indirect evaluations of

Table 8. Application of Criteria - Telecommunications subsector

Services	Direct Assessment (Horizontal Criteria)					Time Criteria		Indirect Assessment (due to dependencies)
	Geographical width	Economic Loss	Human Casualties	Environmental Cons.	Consequences to the Public	Time of consequence manifestation	Recovery Time	
Voice/Data communication services	Territory	Important % of GNP	Potential Loss due to impact on Health Sector	–	Effect on the lives of million citizens	Rapid consequence manifestation	Rapid recovery	Affects most CIs
	LEVEL 3	LEVEL 3 or LEVEL 2	LEVEL 1		LEVEL 3	CATEGORY 2		LEVEL 3
Internet Provision	Territory	Important % of GNP	Potential Loss due to impact on Health Sector	–	Effect on the lives of million citizens	Rapid consequence manifestation	Rapid recovery	Affects most CIs
	LEVEL 3	LEVEL 3 or LEVEL 2	LEVEL 1		LEVEL 3	CATEGORY 2		LEVEL 3

dependencies. The Communications sub-sector services depend to a large extent, from a single provider (OTE).

- Concerning the temporal analysis of impact, it was shown that both the voice/data communication services and the provision of Internet services present fast impact effects but rapid recovery times, thus fall within the same priority level.

Acknowledgments. This work was performed within the *OLIKY* project framework. OLIKY was coordinated by the INFOSEC Laboratory (Athens University of Economics & Business) and funded by *diaNEOsis*, a non-government and non-profit research and analysis organization, located in Greece. The opinions expressed herein are those of the authors.

References

1. EU Commission: Communication from the Commission on a European Programme for Critical Infrastructure Protection COM (2006) 786 final (2006)
2. EU Commission: European Commission, staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP), Brussels (2012)
3. EU Commission: European Commission, staff working document on a new approach to the European Programme for Critical Infrastructure Protection making European Critical Infrastructures more secure), Brussels, Belgium (2013)
4. EU Commission 149: European Commission. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience (2009)
5. EU Council: Council of the European Union, Non-Binding Guidelines for the application of the Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, Brussels [14808/08] (2008b)
6. EU Council: Proposal for a COUNCIL DECISION on a Critical Infrastructure Warning Information Network (CIWIN). COM (2008) 676 final (2008c)
7. ENISA, Mattioli, R., Levy-Bencheton, C.: Methodologies for the identification of Critical Information Infrastructure assets and services. ENISA Report, December 2014 (2014)

8. Faily, S., Stergiopoulos, G., Katos, V., Gritzalis, D.: "Water, Water, Every Where": nuances for a water industry critical infrastructure specification exemplar. In: Rome, E., Theocharidou, M., Wolthusen, S. (eds.) CRITIS 2015. LNCS, vol. 9578, pp. 243–246. Springer, Cham (2016). doi:10.1007/978-3-319-33331-1_20
9. FC: Federal council's basic strategy for critical infrastructure protection, basis for the national critical infrastructure protection strategy. In: Confédération Swisse, 18 May 2009 (2009)
10. French Strategy: French national digital security strategy. French Republic (2015)
11. FRG: National Strategy for Critical Infrastructure Protection (CIP Strategy). Federal Ministry of the Interior, Federal Republic of Germany. Berlin, June 17 2009
12. Klaver, M., Luiijf, H., Nieuwenhuijsen, A.: RECIPE: Good practices manual for CIP policies, for policy makers in Europe (2011)
13. Kotzanikolaou, P., Theocharidou, M., Gritzalis, D.: Accessing n-order dependencies between critical infrastructures. Int. J. Crit. Infrastruct. Prot. **9**(1–2), 93–110 (2013)
14. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D.: Cascading effects of common-cause failures in critical infrastructures. In: Butts, J., Shenoi, S. (eds.) ICCIP 2013. IAICT, vol. 417, pp. 171–182. Springer, Heidelberg (2013). doi:10.1007/978-3-642-45330-4_12
15. Kotzanikolaou, P., Theoharidou, M., Gritzalis, D.: Interdependencies between critical infrastructures: analyzing the risk of cascading effects. In: Bologna, S., Hämmerli, B., Gritzalis, D., Wolthusen, S. (eds.) CRITIS 2011. LNCS, vol. 6983, pp. 104–115. Springer, Heidelberg (2013). doi:10.1007/978-3-642-41476-3_9
16. Lebau-Marianna, D., Roger, E.: France – three decrees reinforced the safety obligations of Operators of Vital Importance, 8 July 2015
17. Livre Blanc: Défense et sécurité nationale, République Francaise (2013)
18. Luiijf, E., Burger, H., Klaver, M.: Critical infrastructure protection in the Netherlands: a quick-scan. In: EICAR Conference Best Paper Proceedings (Vol. 19). Denmark (2003)
19. MSB: A first step towards a national risk assessment. Swedish Civil Contingencies Agency-MSB, Sweden (2011). 2011
20. MSB: Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure. Swedish Civil Contingencies Agency, Risk & Vulnerability Reduction Department (2014)
21. Renda, A., Hammerli, B. (2010). Protecting critical infrastructure in the EU. CEPS Task Force Report
22. Salonikias, S., Mavridis, I., Gritzalis, D.: Access control issues in utilizing fog computing for transport infrastructure. In: Rome, E., Theocharidou, M., Wolthusen, S. (eds.) CRITIS 2015. LNCS, vol. 9578, pp. 15–26. Springer, Cham (2016). doi:10.1007/978-3-319-33331-1_2
23. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Gritzalis, D.: Risk mitigation strategies for critical infrastructures based on graph centrality analysis. Int. J. Crit. Infrastruct. Prot. **10**, 34–44 (2015)
24. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Lykou, G., Gritzalis, D.: Time-base critical infrastructure dependency analysis for large-scale and cross-sectoral failures. Int. J. Crit. Infrastruct. Prot. **12**, 46–60 (2016)
25. Theocharidou, M., Kandias, M., Gritzalis, D.: Securing transportation-critical infrastructures: trends and perspectives. In: Georgiadis, C.K., Jahankhani, H., Pimenidis, E., Bashroush, R., Al-Nemrat, A. (eds.) Global Security, Safety and Sustainability & e-Democracy. LNICST, vol. 99, pp. 171–178. Springer, Berlin, Heidelberg (2012). doi:10.1007/978-3-642-33448-1_24
26. UK: Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards (2010)

http://www.springer.com/978-3-319-61436-6

Security of Industrial Control Systems and
Cyber-Physical Systems
Second International Workshop, CyberICPS 2016,
Heraklion, Crete, Greece, September 26-30, 2016,
Revised Selected Papers
Cuppens-Boulahia, N.; Lambrinoudakis, C.; Cuppens, F.;
Katsikas, S.K. (Eds.)
2017, VII, 121 p. 19 illus., Softcover
ISBN: 978-3-319-61436-6