UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Luis Carlos Herrera Velasquez

A Comprehensive Instrument for Identifying Critical Information Infrastructure Services

Master's Thesis (30 ECTS)

Supervisor: Olaf Manuel Maennel, Ph.D.
Co-supervisor: Raimundas Matulevičius, Ph.D.

Tartu 2016

A Comprehensive Instrument for Identifying Critical Information Infrastructure Services

Abstract:

The identification of Critical Information Infrastructure (CII) services has become a top priority for governments and organizations, and a crucial component of a sound cyber security policy. As the interconnectivity of essential services spreads, the probability of disruptions increases and with it the vulnerability of all Critical Infrastructure (CI) sectors public and private. The impact of an undue interruption of essential services may develop in a devastating cascading effect and the collapse of a country's infrastructures system. The purpose of this work is to introduce an original comprehensive instrument that supports the escalated identification of CII services on the basis of three analytical components: the identification of main stakeholders, as an accurate terminology for establishing a common understanding of the terms; the calculating process for criticality ranking that works as an adaptable matrix; and, an illustrative framework called the 360-DEGREE-FEEDBACK that applies the complete perspective. Terminological development preceded the formulation of the instrument considering preliminary findings on that the field of CII warrants more clarity and precision, and that the CIIs, despite their commonalities with other dimensions of CIs, possess unique characteristics that should be assessed independently. The applicability of the instrument is illustrated in a case study of Colombia, which is used to exemplify the relationship between two potential essential services and map the likely position of them in the table of national protection priorities. This study combines qualitative and quantitative methods, benchmarking theoretical contributions, and relying mainly on documentary analysis, secondary statistical data from official sources, semi-structure interviews and a case study of practical implications. This thesis is written in English and is 56 pages long, including 22 figures and 26 tables.

Keywords:

Critical Information Infrastructure, Critical Infrastructure, Criticality Criteria, Cyber Dependence, Cascading Failure, Information and Communication Technology.

CERCS: P170 Computer science, numerical analysis, systems, control

Kõikehõlmav tööriist kriitilise infotaristu teenuste identifitseerimiseks

Lühikokkuvõte:

Kriitiliste Informatsiooni Infrastruktuuride (KII) teenuste kindlaks määramine on üks valituste ja organisatsioonide peamisi prioriteete. KII on ühtlasi kaaluka küberturvalisuse poliitika kriitiline osa. Nii avalikus kui erasektoris Kriitilise Infrastruktuuri (KI) haavatavus suureneb, sest kasvab omavahel ühilduvate hädavajalike teenuste arv, samaaegselt tõuseb ka tõenäosus vahelesegamisteks. Hädavajalike teenuste lubamatute vahelesegamiste mõju võib välja viia arenguteni, kus aset leiab hävitav kaskaadeffekt, mille tagajärjeks on riikliku infrastruktuurisüsteemi kokkuvarisemine. Antud lõputöö eesmärgiks on tutvustada ainulaadset kõikehõlmavat instrumenti, mis toetab eskaleeritud KII teenuste kindlaksmääramist, ja põhineb kolmel analüütilisel komponendil. Nendeks on: peamiste sidusrühmade kindlaks määramine kui täpne terminoloogia loomaks terminitest ühist arusaama; kohaldatava maatriksina töötav kalkuleerimisprotsess kriitiliste reastuste otstarbeks; ja, illustratiivne raamistik nimega 360-kraadi-tagasiside, mis kinnistab terviklikku lähenemist. Terminoloogiline edasiarendus tuleneb vahendi loomisest, mis võtab arvesse esialgseid leide, see tagab KIIde vallas suurema selguse ja täpsuse. Unikaalseid tunnusjooni omavad KIId peaksid olema hinnatud iseseisvalt. Seda

vaatamata KIIde ühistele joontele KIde teiste tahkudega. Vahendi kohaldatavus on näitlikustatud Kolumbia juhtumikirjelduses, kus on illustreerivalt toodud seos kahe potensiaalse hädavajaliku teenuse vahel. Juhtumikirjedluses on ühtlasi kaardistatud nende tõenäoline paiknemine riikliku kaitse prioriteetide seas. Antud lõputöö kombineerib kvalitatiivseid ja kvantiatiivseid meetodeid, sisaldab võrdlusanalüüsi teoreetilisi sisendite kohta. Lõputöö tugineb peamiselt dokumentide analüüsil, ametlikest kanalitest pärineval sekundaarselt statistilisel infol, poolstruktureeritud intervjuudel ja juhtumikirjeldusel, mis annab tööle praktilise kaalutluse. Käesolev magistritöö on kirjutatud inglise keeles, koosneb 56 leheküljest, 22 näidetest ja 26 tabelitest.

Võtmesõnad:

Kriitiline Informatsiooni Infrastruktuur, Kriitiline Infrastruktuur, Kriitilisuse Kriteerium, Cyberist Sõltumus, Ahel Ebaõnne, Informatsiooni ja Kommunikatsiooni Tehnoloogia.

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

Acknowledgments

I was fortunate to have support from a number of highly knowledgeable persons. First of all, I would like to thank professor Olaf Manuel Maennel, PhD (Tallinn University of Technology) who gave me the courage and help to accomplish it; I definitely owe my achievement to him. Second, thanks to Mrs Galina Danilišina (Councillor of vital services in Estonia) for her guidance during the development of the 360-DEGREE-FEEDBACK framework. Third, recognizes to Professor Maria Claudia Solarte (Tallinn University of Technology) for her advice during the research design. Finally, appreciates to Mrs Rossella Mattioli (ENISA), Mrs Lorena Trinberg (NATO-CCDCOE) and professor Hayretdin Bahsi, PhD (Tallinn University of Technology) for their recommendations and suggestions during my research.

Table of abbreviations and terms

BIA	Business Impact Analysis
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
ENISA	European Union Agency for Network and Information Security
GDP	Gross Domestic Product
GWh	Giga Watt hours
ICT	Information and Communication Technology
IS	Information System
OAS	Organization of American States
NIST	National Institute of Standards and Technology

Table of Contents

List of figures

List of tables

1 Introduction

1.1 Motivation

Future societies depend on the provision of essential services such as electricity, web services, airport operations, etc. These services are often interconnected with each other and rely on Information and Communication Technologies (ICT), termed as cyber dependence. Cyber dependence is fundamental for the proper functioning of Critical Infrastructure (CI). Dependence may be described as: "*the situation in which you need something or someone all the time, especially in order to continue existing or operating*"[1]. Therefore, interdependence is the mutual or bidirectional dependence on each other. Indeed, the connectivity among CIs is classified into four main types of interdependencies: physical, geographic, cyber and logical; and these interdependencies could be disrupted by failures, termed as: escalating, cascading, and common cause [1].

The protection of communication networks has been studied for many years by organizations and professionals in information security. The studies have occurred to prevent and mitigate the impact of cyber attacks. If a network is compromised by malware, this tends to lead to the spread of further viruses [2], which once spread is very difficult to stop. This can happen because electronic devices are vulnerable to malware attacks; common human errors such as system misconfiguration or disclosure of classified information [3]; increase disruption to the systems and, the growing interconnectivity that facilitates the propagation of these [4].

Researchers have shown that cyber dependence not only brings benefits like information sharing, but also increases the probability of disruptions, that could impact people's lives, the economy of countries, and its essential services supply [5]. Therefore, the identification of CII services is the first step in the process to protect the interests of communities who depend upon services such as these.

Some countries have developed their own methodology for the identification of CII services; methods are required to be as precise as possible in determining what must be protected [6]. In Estonia, for example, the definition speaks of vital services instead of critical sectors, with more than 40 vital services and 160 providers identified[2]; Italy has identified only two critical sectors: energy and transportation [7]; France used the "Operator-based" approach to identify 12 critical sectors, 21 subsectors and 220 vital operators; Switzerland used a "Service-oriented" approach to identify 10 critical sectors and 28 sub-sectors; and, The United Kingdom uses the "Asset-based" that is a hybrid between the "Service-based" and the "Operated-based" approaches [5].

1.2 Problem statement

Although the existence of standardization efforts and organizations devoted to the identification and protection of CII services exist in the European Union. Members do not apply the same approaches and frameworks. Strategies differ and regulations are based on specific factors as the culture, geography, habits, particular hazards, religion, priorities and responsibilities. Nevertheless, the individual approaches members have used for the identification of the CII services, has led governments to allocate resources and rationalize efforts to increase their cyber security capacity. One such program is the CII protection plan that contains resource allocation and policies for the prevention and mitigation of

[1] Cambridge dictionaries online. Viewed on 02-Jan-16. Retrieved from http://dictionary.cambridge.org
[2] Retrieved by personal interview (2015, December 15). Interviewer Code: ID_9

unauthorized access to information; and, modification or destruction of software that is required by the CI to work properly [8].

Countries such as Colombia that have not yet defined CI categories [9], would benefit from the development of a comprehensive instrument that could be used to gather the information from public and private operators. Comprehensive may be understood as: including everything that could be necessary[3]. Otherwise, to take one or part of these existing methodologies from industrialized nations that have not the same economy, resources: human, time and technical, or sectors, like: space and research, chemical and nuclear industry, etc., and apply to a country such as Colombia, would not be appropriate or suitable for protecting their essential services.

In 2014, Cyber Security Technical Assistance Mission (CSTAM) developed a meeting with more than 20 experts in cyber security from different countries in order to analyse of the status of cyber security. It was established and affirmed that Colombia has not defined what its critical infrastructure is, as yet, and therefore is unable to define what to protect [9]. However, one year later, in 2015 the OAS released a report with dangerous information of the current state of cyber security, in which was affirmed that cyber threats in Colombia are growing and a great amount of phishing, computer hijacking, identity theft, among them, running in Latin America is executed from this country [10]. These statements corroborate that Colombia, at least, needs to define and identify their CI and essential services in order to develop a protection plan to enhance their cyber security.

The following example illustrates the importance of CII services in Colombia and the possible consequences caused by a cyber attack on one of their essential services. The aeronautical agency reported that in 2014 the domestic aviation carried a total of 36,134,568 passengers[4]. That means if someone executes a cyber attack against the air navigation services, this would stop all air traffic, and the malfunction would significantly affect the population in Colombia. In addition, cyber dependence could disturb other vital services as airports operation, meteorological monitoring, food distribution, etc.

1.3 Main goal

In order to support countries as Colombia that have not yet identified their essential services, this thesis aims to develop a comprehensive instrument for identifying CII services and offers a common ground in terminology that facilitates the communication between government and the public/private sectors. As well, it illustrates a proposed framework that describes the flow of information among principal stakeholders, which are proposed as a result of a literature review. Framework is understood as "*a system of rules, ideas, or beliefs that is used to plan or decide something*" [5].

Research Question: How to develop a comprehensive instrument for identifying critical information infrastructure services?

Research Tasks:

1) Based on research papers and secondary statistical data to establish the national stakeholders for the CII that facilitates the communication among them;
2) To analyse existing guidelines and gathered information from expert to establish the criticality criteria for the identification of CII services;

[3] Cambridge dictionaries online. Op. cit.
[4] Aeronautical Civil. (2014). Operational statistics of the Colombian aviation. Viewed on 02-Feb-16. Retrieved from http://goo.gl/04BzEm
[5] Cambridge dictionaries online. Op. cit.

3) To illustrate a proposed framework that describes the flow of information between stakeholders for the identification of critical services.

1.4 Scope

This instrument does not intend to display a list of CII services of any country. On the contrary, this research offers an alternative instrument that could be used for collecting relevant information to identify those essential services that its core activity relies on ICT. Although, this work is based on secondary statistical data of Colombia in order to exemplify a particular case and to pinpoint some generic criticality criteria, it is available for governments and stakeholders that have not yet identified their CII services.

1.5 Research design

This work includes a combination of qualitative and quantitative methodologies, applying throughout the following methods: document analysis (qualitative) for collection and analysis of research and academic papers, public documents and existing guidelines/methodologies as contributions to identify CII services. Semi-structured Interviews are presented (qualitative) to understand the vision and plot an overview that draws from the expertise of professionals in the field (there are 17 experts whose interviews represent a specific and accurate knowledge base in CII). Secondary statistical data from official sources (quantitative) are examined and presented with pre-existing numerical data that contributes to answer the research question and determine the relationships and specific factors among Internet users, financial resources, cyber attacks data, etc., [11]. As a result of the analysis, this instrument establishes an alternative definition about CII services, a generic criticality criteria and a proposed illustration that describes the flow of information between principal stakeholders, using secondary statistical data from the country of Colombia.

1.6 Thesis structure

This work includes five main chapters. As is displayed below:

The fists part consists of background information, which explores and examines more than 20 research papers and guideline manuals released by countries such as The United States, Germany, France and Estonia. These countries had already identified their essential services and also held an accurate protection plan. This chapter shows the importance of essential services for society and how communication networks have become a top priority for governments and organizations.

The second part focuses on the identification of stakeholders, which could help governments to design roles in national policies and guidelines that would allow for the distribution of tasks and also to strategize efforts to identify CII services. It is classified in three layers:

1) National decision makers;
2) Strategic operators;
3) Collaborating institutions.

Although, criticality criteria could be a political decision in most countries, their applicability includes academic, administrative and technical issue. For that reason, the third part suggests a procedure for the enumeration of the table of protection priorities. Criticality criteria can be calculated by two influences: importance and risk, which is the result of crossing threat, vulnerability and consequence [12]. Based on the expertise of 17 professionals in the field and guidelines released by countries as The United States and

European Union, the following criticality criteria and factors are established as a generic list:

Criteria

1) Public health and safety impact;
2) Economy impact;
3) Psychological impact;
4) Political/Governance impact;
5) Dependence impact.

Factors

1) Effects of time;
2) Magnitude;
3) Scope distribution.

The fourth part is by using the 360-DEGREE-FEEDBACK framework, which can collect data from principal stakeholders, this is an illustrating flow of information that contains eight specific steps, and these are:

1) Set goals and policies;
2) Identify CII operators;
3) Establish criticality criteria;
4) Apply a BIA and risk assessment;
5) Identify CII services;
6) Report continuity plan;
7) Identify cyber dependencies;
8) List CII services, operators and sectors.

This framework is viable and can be possible, because once the CII services are identified; each essential service contains the path travelled during the process, such as: CII service, operator, subsector and sector, and on-going interaction among the main stakeholders; in order to keep continues communication that allows exchanging information and resources.

The last part of this research called as the case study of Colombia, it is based on some secondary statistical information of Colombia; the case's description represents the analysis of behaviour of potential CII services. Nonetheless, this illustration does not pretend to display a real list of Colombia' CII services because the criticality criteria ranking does not belong to the state's characteristics. On the contrary, this hypothetical scenario is used to exemplify the relationship between two essential services and map the likely position of them in the table of national protection priorities.

2 Background

Information System (IS) research is a discipline that includes qualitative and quantitative methods, this approach explains the relationship between people and social aspects within an organization as a system, and how it is supported by the use of computer technology [13] [14]. In other words, this discipline could be considered as a link between society and information and communication networks. On the one hand, information can be as important as other business assets, and communication networks have become a top priority for organizations because these not only have to offer access information 24 hours a day to users, but also the use of this can reduce operating costs, transaction time and overheads [15]; turning it into an attractive target for cyber attackers. As a result, organizations have to ensure that their information is protected against people who do not have the right to access specific data [8]. On the other hand, society depends increasingly on the national Critical Infrastructure (CI) that offers essential services as water distribution, web services, bus services, etc., which are obliged to support the government in providing a high quality and a readily available system of services. Actually, in the past few years' organizations have purposefully increased interconnection between CIs to share resources and efforts [7].

Therefore, economy and society depend on the proper functionality of CIs [16]; these infrastructures are interdependent, which implies that the state of one can directly influence others [1][17][18]. There are 4 types of interconnection among infrastructures; however, these interdependencies are not necessarily mutually exclusive, these are [1][18]:

1) Cyber interdependence: of which the core activity is based on the proper functioning of information and communication networks;
2) Physical interdependence: where two or more infrastructures are physically interdependent if a product produced by an infrastructure (output) is strictly necessary by another infrastructure for it to operate properly (input);
3) Geographical interdependence: this occurs when physical components of one or more infrastructures are sharing a spatial proximity, this type of interdependence is mainly affected by physical damage such as terrorism or natural disasters;
4) Logical interdependence: where two or more infrastructures are logically interdependent if the state of each infrastructure depends on the state of the other through a different mechanism to the above interdependencies. An example of logical interdependence is when airfare to a specific city is a discount; this allows more people to travel to that destination and the hotel sector increase its reserves. In this case, the interdependence is due to human actions and is not the result of a physical, geographic or cyber interdependence.

In 2008, research surrounding 4 types of interdependencies showed that telecommunications and electricity are the most important infrastructures that support infrastructure interdependence. Furthermore research indicated, "*critical infrastructures face a twofold threat from both technical and social vulnerabilities*" [4]. In support of this, Estonia is much more accurate to say that their vital services are based on three pillars: communication, data processing and energy; 90% of its services are dependent on information technologies; which means that if there is an interruption of IT, the service is also greatly affected[6]. This clearly illustrates the strong influence of electricity and the

[6] Director General of the Estonian Information System's Authority. (2013). Viewed on 18-Mar-16. Retrieved from https://goo.gl/S0yqZ9

Information and Communication Technology (ICT) on the proper functioning of society. As described in the following table:

Table 1. List of CI sectors and definitions established by some countries

	Definition of CI	Total of sectors
The United States	"Assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" [19][20][21]**.**	Financial services; chemical; communication; commercial facilities; dams; emergency services; critical manufacturing, defence industrial base; healthcare and public health; energy; government facilities; information technology; transportation; food and agriculture; nuclear reactors, materials and waste; and, water and wastewater systems. Total: 16 CI sectors
European Union	"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" [19][22][23].	Energy; Information, Communication Technologies; Water; Food; Health; Financial; Public & Legal Order and Safety; Civil Administration; Transport; Chemical and Nuclear Industry; Space and Research. Total: 11 CI sectors
Germany	"CIs are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences" [24].	Energy; information technology and telecommunication; transport; health; water; food; financial and insurance; state and administration; and, media and culture. Total: 9 CI sectors

In order to understand the relationship between CI sectors and CII services, and avoid overlap in these terms, this chapter explains each definition separately.

Although, some of the above examples refer to sectors as energy, transport, water, food, etc., which provide the essential services that support modern information societies and economies; the difference between these countries is that the United States has 7 CI sectors more than Germany, which corroborates that not only the definition cannot be universally applied in the same way and that there is no universally recognized meaning of what CI is, but also their approaches and interests are differ according to region.

Consequently, CII is part of the organizations that are based on the correct operation of ICT, which leads to a correct functioning of society [7]. Protecting the entire networks has always been problematic and unreachable. These factors make it more difficult to know

how and what must be protected. In order to understand the definition of CII, three questions need to be examined:

1) What should be termed as critical?
2) What does the information mean in this context?
3) What does the infrastructure mean?

Firstly, critical should be understood as: "*Of the greatest importance to the way things might happen*"[7]. However, it can be also be defined as an essential contribution to society in order to have a minimum quality level of international and national law; economy; public health and safety; and, ecological environment [25]. From the previous statements critical could be understood as a large number of factors that contribute to the lives of people, the economy of a whole country; that is one of the reasons why organizations devoted to the identification and protection of CII services apply the criticality criteria to their services, which can be widely organized by critical proportion, critical time and critical quality [12].

Secondly, although some research and public papers related to CII did not define or arrive at a universal criterion for CII, it is accepted that communication networks have a vital role to play. For example, professor Nickolov says that communication technologies are stimulating globalization, and improve the efficiency, productivity and competitiveness of the organizations [8]. Guidelines released by the organization ENISA, state that communication networks are a meaningful part of the lives of European citizens, and they symbolize the fabric of the future information [7].

There are other definitions in published documents that explain what an Information System may also be. To be as precise as possible, it was defined as interrelated systems working together to collect, process and store data to help to analysis, decision-making and visualizations of organizations [26]. Similarly defining the Information System as computer-based systems, which are combined of software, hardware and telecommunications networks to collect, create and distribute useful information [27]; and, in 2014, one researcher specified that an Information System is the vital component that produces information which may be perceived as five main factors: software, hardware, data, people and procedures [28]. According to these definitions and under the CI's context, the word information is related with communication networks that could be constituted as a combination of the telecommunication, hardware and software in order to storing/processing/exchange data along network links, which may be subject to risks that may have unfavourable consequences on the functioning of the organization by compromising the availability, confidentiality, or integrity of information.

Thirdly, infrastructure is defined as "*the basic systems and services, such as transport and power supplies, that a country or organization uses in order to work effectively*"[8], the Oxford dictionaries online defines this as "*The basic physical and organizational structures and facilities, e.g. buildings, roads, power supplies; needed for the operation of a society or enterprise, water and power lines, and public institutions including schools, post offices, and prisons*"[9]. These terms support the definition in the field of CI, both the Professor Wilde and Rinaldi based their researches on the definition established by the Critical Infrastructure Assurance Office (CIAO) [1][18][21].

[7] Cambridge dictionaries online. Op. cit.
[8] Cambridge dictionaries online. Op. cit.
[9] Oxford dictionaries online. Viewed on 02-Jan-16. Retrieved from http://www.oxforddictionaries.com

Nonetheless, the professor Tabansky has stated that infrastructure is a system with several facilities to carry out activities and argues that it would be considered critical when the disruption causes a significant socio-economic crisis; three factors can define an infrastructure as critical [16]:

1) The symbolic importance in the country, such as museums and monuments;
2) The direct dependence on infrastructures like energy and telecommunication networks;
3) The interconnectivity among other infrastructures that could cause cascading failures.

Understanding the definitions of CI and CII are often still unclear [29], and some research papers have a lack of clarity about the relationship between them, which is illustrated in the following statements: In Italy the Protecting National Critical Infrastructure from Cyber Threats – TENACE project makes a distinction between cyber and physical CI, classified as physical a wide range of facilities and system: energy, transportation, etc.; and, cyber as intangible and tied to information technology: financial services, e-government, etc. [30].

In addition, professor Wilde matched with the TENACE project, which argues that the cyber infrastructure is as important as physical infrastructure [18]. Quite the opposite, Estonia says of the CIIs are a part of the CI, even though their definition speaks of vital services instead of CI sectors[10]. And, in contrast, Lithuania defined it, as: "*Critical information infrastructure shall mean an electronic communications network, information system or a group of information systems where an incident that occurs causes or may cause grave damage to national security, national economy or social wellbeing*" [31].

As a result of the above definitions, CII is considered as a part of national CI and sequentially society; but it should be analysed as a whole system in order to avoid misunderstandings with their definitions and applicability. As shown in the following figure:

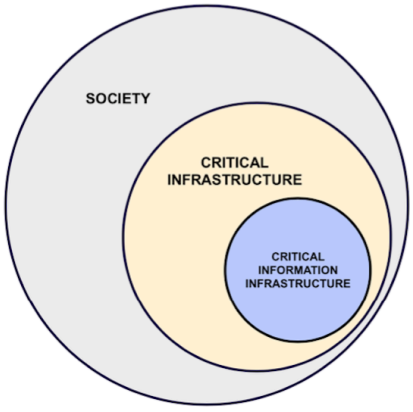

Figure 1. Critical Information Infrastructure as a system.

Continuing the concept of CII services, there are different methodological approaches that are used by European Union members. In 2014, ENISA released a methodology for the identification of CII assets and services based on collected information from some member states, that paper provided a list of 11 CI sectors and highlighted that not all sectors are important for all country. ENISA identified two approaches:

[10] Republic of Estonia – Information System Authority. Viewed on 05-Feb-16. Retrieved from https://www.ria.ee/en/ciip.html

Firstly, a non-critical service dependent approach: Network architecture analysis, which is a methodology that is not used by any country in Europe, but that private companies use to map their networks. This approach includes:

1) "*The analysis of the IP and data network, the traffic load patterns, and failure patterns*" [7];
2) "*The identification of components, which are critical to the operation of the overall network or a major part of the network*" [7].

This approach identifies the core network and some additional components of an organization that support most of the data traffic to generate a global map. However, one disadvantage is that both the public and private sectors must design a complete map of the network architecture and ignore critical services, which are interconnected through ICTs, because it is based specifically on the network infrastructure as a whole. And, another disadvantage is that the analysis of a large map of infrastructure may neglect to include components that are at lower levels, but could also be considered as critical.

Secondly, a Critical Service (CS)-dependent approach, as is present in this methodology, ENISA included 3 main steps to work with, and these are:

1) Identification of the critical sector, in this step, member states have already identified a list of CI sectors. Nonetheless, if another country outside the European Union wanted to use this methodology, it could not fully apply the criterion as this step was omitted;
2) Identification of critical services, is divided into two sub-approaches, each depends on who is responsible for identifying critical services:
   a. The state-driven approach or critical service-driven, where the responsibility is taken by government agencies, who is responsible for identifying the critical sectors and the list of essential services, which are found by applying criticality criteria. Then, the government selects the operators that are responsible for providing these essential services;
   b. The operator-driven approach or vital operator, in this approach, government is also responsible for identifying the CI sectors. Then, they select a list of operators instead of essential services, who are responsible to identify CII assets and services. Each sub-approach has advantages and disadvantages [7], which are shown in the following table.

Table 2. Contrast of sub approaches described by ENISA.

	The state-driven approach	**The operator-driven approach**
Advantages	1. The government approves and audits the CII protection plans per each service, which can ensure a comprehensive plan; 2. The government is directly responsible for the national economy and welfare of its people. The government have overall control of the protection of CII services ensures these factors; 3. The list of criticality criteria is focused on national interests.	1. The government approves and audits the CII protection plans per each service, which can ensure a comprehensive plan; 2. The operators can establish the cyber interdependencies between their institutional CI services; 3. The operator has resources that to locate and identify their critical services.

Disadvantages	1. The government has to allocate adequate resources (human, financial and time) for accomplishing the final purpose; 2. If the list of essential services is not selected properly, it could disfigure the real interests of society; 3. The government uniquely responsible for the identification of CI sector and CII services. Operators do not participate in this process and their responsibilities are aimed at establishing a CII protection plan and deploying said plan; 4. There is no coordination among CI sectors. Therefore, the cyber interdependencies could be established incorrectly.	1. The government represented by each ministry decides whether the operator is part of CI sector; 2. Criticality criteria can focus on needs of the business' operator instead of countries national interests; 3. The operator is the sole decider of what services will be part of the CII; 4. It is a non-homogeneous deployment of the identification of CII services, and the meaning of essential services could be confused.

The last step in this process is the identification of critical information infrastructure network assets and services supporting critical services. The CII services and assets are supported by some criticality criteria. This classification represents the final phase of that methodology, where each operator establishes the respective protection plan for each service.

Regardless of the approach, ENISA argues that success would be to establish good communication and cooperation among stakeholders involved in the operations of CII services. Researchers go beyond this, adding that success must also include factors like transparency in national systems, social and industrial awareness, public-private cooperation and well-defined job distribution [15]. Nonetheless, ENISA catalogued the task responsibly, and stated they are: operators of CI and network operators (electronic communication providers, national telecommunication regulator and cyber-security agencies). Other research reference participatory factors at 3 levels: technological, operational, and national-strategic [16].

In addition, the correct knowledge distribution is vital. This is a factor that involves CI, stakeholders and the decision makers at all levels, key is the relationship among them, which can protect or damage dependent on methods of knowledge sharing and distribution. Both professor Rinaldi and Tabansky classified these types of failure, as [1][16]:

1) A common cause failure by earthquakes, floods and fires; this failure is not related with cyber interdependence, however it could affect the normal behaviour because a single incident can damage others services;
2) A cascading failure: this is a good example of the result of a successful cyber attack, because the disruption of one service could cause the failure in other services even if they have no directly cyber dependence [32]. In fact, a real modelling could be demonstrated that "*a failure of one node in a network may lead to a cascade of failures in the entire system*", this was a result of simulation of the real geographical locations, using real-world data from a power network, the case of Italy [33];
3) An escalating failure: this is related to time and severity, which can rapidly increase the damage and recovery becomes more complex if it is not stopped on time [16][34].

Appropriately, in order to prevent and mitigate those failures, industrialized countries have employed criticality criteria to establish a range of infrastructures to classify protection priorities [35]. Although, there is a group of criteria typically used to evaluate the impact of social vulnerability, economic damage assessments, capabilities and resilience studies; the definition of terms like resiliencies, risks, vulnerabilities and criticality are still not 100% clear [12][32].

On the one hand, some research papers propose a combination of the Business Impact Analysis (BIA) and risks assessment in order to understand more broadly the correlation of the essential services and potential threats, vulnerabilities and consequences [36]. The main task of BIA is to identify the important essential services and to understand the impact and effect the disruption or failures of these processes have on a company [37]. Actually, the National Institute of Standards and Technology (NIST) defined it, as: "*The BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components*" [38].

On the other hand, professors Theoharidou, Kotzanikolaou and Gritzalis think that the lack of clarity is to define the correlation between "*the protection of CIs and the mitigation of security risks faced by CIs*" [35]. Nevertheless, some researchers and interviewees suggest that criteria could be summarised in "*how serious is serious*" and the criteria could be based on the major detrimental impact on economic, social consequences and to loss of life [10][15]. In 2014, ENISA suggested criticality criteria on: populations affected; concentration; economic impact; international relations; public order; public confidence; and, public operations hindered and how 3rd party MS services are affected. On the other hand, the United States catalogues the criticality criteria on: economic, public health and safety, psychological, and governance/mission[11].

2.1 Conclusion

The identification of CII services play a meaningful role for the welfare of people as it allows the governments to identify what essential services and cyber dependencies must be protected [6]. For that reason, countries like The United States, Germany, France, Estonia, among others, have already identified these essential services and have an accurate protection plan that includes the detailed description of specific relevant elements. Nonetheless, these countries not only do not share the same definitions or an agreed universal criterion, and their approaches and interests differ, this is primarily because of states do not have the same economy, resources and/or sectors; which influences significantly in the direct dependencies on other infrastructures and people's lives. Each country is unique and thus its needs are not equal.

Independently and separate from existing criticality criteria (based on population, economic, interdependence, international relations, defence, public order, etc.), CII services could be mapped via the impacts which could then be calculated based on 3 universal characteristics [12][35]:

1) Scope distribution: the geographic area that could be affected by the unavailability of a specific CI;
2) Magnitude: the effects of gravity are caused by the interruption of a particular CI;
3) Effects of time: it is represented in hours, days, months and years, which is the point that the loss of an element could have a grave impact.

[11] National Infrastructure Protection Plan. (2009). The United States. Viewed on 10-Feb-16. Retrieved from https://goo.gl/4oOb6a

3 Main Stakeholders

Due to the lack of clarity in published research papers, and no universally accepted solution for the identification of CII services [7][29] as discussed in the previous chapter it is important to define what we understand as CII. To identify the national stakeholders and define an accurate terminology for establishing a common understanding of the terms of CII is one the bases to distribute tasks, transmit feedback in order to avoid unnecessary efforts. Therefore, this chapter proposes a helpful definition that facilitates the communication among principal stakeholders.

3.1 National stakeholders

First of all, a global description of the national stakeholders involved in the identification of CII services lead to define precisely the minimum terminology that could be used for this purpose. In order to offer an alternative methodology, this section hierarchically organises the national stakeholders to make it easier to interpret and to avoid unnecessary confusion and effort, which has been the result of existing approaches like operator-base and service-based; research papers; as seen in contributions made by interviewees; and, guidelines released by ENISA, NIST, and the OAS.

The national stakeholders are proposed into 3 types of layers:

1) National decision makers are the leaders responsible for the determination of CII operators based on all sectors, such as regulatory bodies, advisory agencies, and/or delegates from each ministry. As well, it could be supported by the national CERT;
2) Strategic operators are responsible for operating and identifying the specific CII services that meet with the criticality criteria established by the national decision makers. In addition, operators must identify the vulnerabilities and risk of their assets and systems, and report periodically to national decision makers the impact and the probability of the occurrence of these threats [39];
3) Collaborating institutions are responsible for analysing cyber dependencies among CII services; to be a coordinator between operators; and, carry out researches and developments to review periodically the identification of new CII services, such as CERTs, organizations devoted to released guidelines for protecting CII (I.e. ENISA, OAS, etc.), and universities that contain professionals in information security, laboratories and financial resources for research.

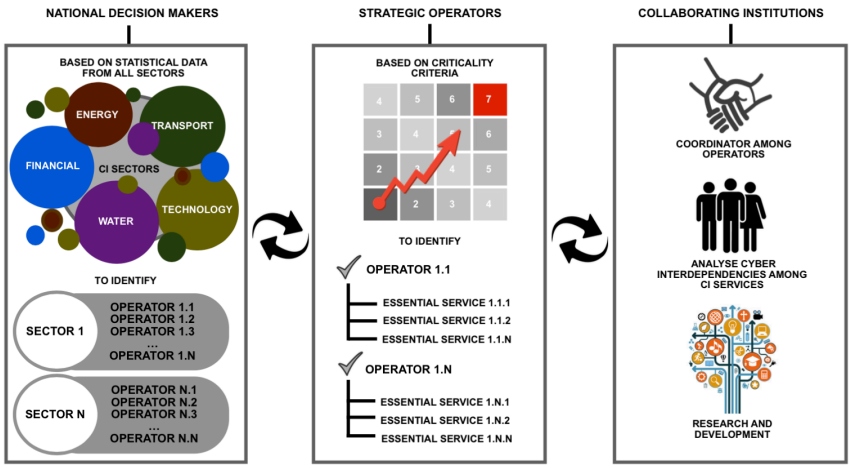

Figure 2. The national stakeholders for the identification of CII services.

First, national decision makers tend to follow global steps based on the operator approach by France, where the state is responsible for identifying CII operators, but the methodology for carrying out their tasks are different, especially the way how operators are enumerated. To describe this process, government is represented by ministries or whoever takes responsibility for this role. They are responsible for identifying CII operators based on statistical data generated by public and private organizations; like loss of human life, users of Internet, financial resources and cyber attacks data; ensuring that all essential services are taken into account, regardless if they belong or not to CI sector; under the concept described in the previous chapter, where CII is considered as a complete system. This differs from the Switzerland's approach, whereby the government is responsible to establish criticality criteria to encourage each operator to use a non-homogeneous deployment as criteria, and to preserve the national interest in order for it to prevail over business interest. Business is understood as any collective private activities that humans carry out to generate value [28][40]. The national decision makers could be supported by the national CERT and composed of regulatory bodies, and/ or delegates from each ministry and advisory agencies.

These responsibilities are assigned to national decision makers layer, because of:

1) Countries as The United States, England and Germany consider that most of the cyber attacks against public and private sectors are demarcated as criminal acts and espionage [41][42]. In other words, these cyber attacks are performed against the interests of the state;
2) Government is solely responsible for establishing guidelines and policies for the identification and protection of national CII not only because it is part of national security measures [15][41], but also the suitable functioning affects all areas of citizens' life [1][16];
3) The principal objective of a national CERT is to protect economic security and the ability of CI [43]. In the case of Colombia, the responsibility for identifying the country's CI was assigned to Colombia's CERT [10].

Second, strategic operators are represented by each provider from all public-private sectors [43], whose main objective is to identify the specific CII services related to generic criticality criteria established by using its own security framework, or a combination of business impact analysis and risk assessment, because:

1) The operators can establish cyber dependencies between their organizational CI services [7]. This process can reveal in their strengths and limitations as an interconnected network;
2) Organizations focus on service delivery and know their internal processes [1], which allows description and identification of essential services faster than other external agency. Actually, in countries such as The United States, 85% of CI is owned by the private sector [18]. In Germany almost 90% of national CI's are in the hands of private companies [15]. In the case of Latin American, 80% of the CI that administers essential services is operated by the private sector [10];
3) Private companies may be reluctant to share their proprietary data, databases and physical files [1]. Although, each operator is able to access to the source, they do not need to report detailed risk assessment to national decision makers; a comprehensive business continuity plan of high level is enough;
4) In 2014, a study carried out by Symantec Lab[12] showed that in Latin American the cyber attacks caused the loss on average of US$2 million per private company.

[12] CONPES document. (2011). Republic of Colombia. P. 7. Viewed on 10-Feb-16. Retrieved from http://goo.gl/a3ZrrC

Therefore, the private sector may offer special expertise and allocate technological and financial resources to protect their services against cyber attacks [7].

Operators must generate a business continuity plan and focused treatment plans of essential services during and after interruptions, to be analysed by the national CERT and collaborating institutions in order to classify potential threats and vulnerabilities These plans also calculate the impact of these occurrences on society and other essential services [39].

Third**,** collaborating institutions: The existing organizations devoted to enhancing the protection of CII's are important parts of the identification of CII services; they can facilitate the coordination and communication among organizations (CII operators). ENISA in Europe release reports and guidelines that emphasise good practices, that protect CII services and help raising awareness on related cyber security challenges. Similarly, the Inter-American Telecommunications Commission represents the OAS, whose main objective is to facilitate and promote the continuous development of ICT. To illustrate this point, in Colombia almost 17 million of users have Internet access[13], this methodology proposes that Internet service providers and telecommunication network operators are perceived as collaborating institutions because these qualify as one of the best options to identify and subsequently handle a cyber attack.

On the other hand, universities could advise on the functionality of the national CERT, because it could improve technical competence without investing too much in terms of resource. Supported by the following arguments:

1) The CERT could be responsible to identify and monitor incidents that affect the national CII, including their essential services [43]. Academic university networks could carry out technical research projects in an efficient and specialised manner [6];
2) Due to malware it is difficult to detect/stop threats when there is interconnectivity with other systems [4]. University researchers, professors, and students could be trained to handle complex research methods to identify threats in the field of ICT [6];

In the case of Colombia, universities are highly valued; two universities are rated academically on the list of 300 best in the world[14]. These universities would be best placed to adequately implement research projects. This ranking is based on indicators such as reputation among the global academic community, its research impact, number of research projects, etc.

3.2 Critical Information Infrastructure Services

Each country establishes their own definition of CII depending on the national needs [15]. The following figure illustrates a clear conception of what CII is and their associated services in this research paper, which is a combination of the definitions of Estonia and Lithuania, and Rinaldi's research paper [1]. Accordingly, CII services are described in this work as: the essential services that belong to the CI and its core processes depend on ICT, which may be interconnected with each other; called: cyber dependent; and that a disruption so such services would inevitably affects other services.

[13] Ministry of Telecommunications. (2015). Statistical data of Colombia. Viewed on 08-Mar-16. Retrieved from http://goo.gl/SCtW6D
[14] QS Top Universities. (2016). Viewed on 15-Mar-16. Retrieved from http://goo.gl/mmIACv

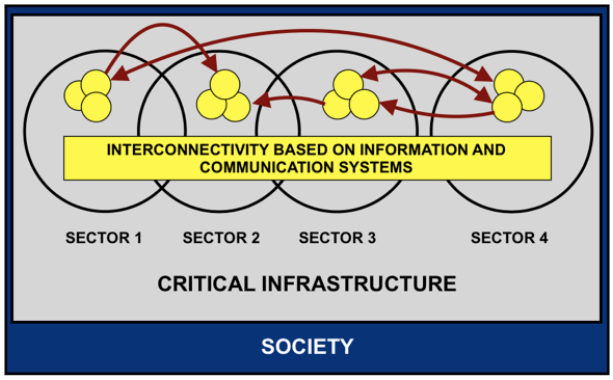

Figure 3. Illustration of the relationship among society, CI and CII services.

Illustrated in fig. 3, the yellow circles represent CII services and the red arrows are the possible cyber dependencies; these yellow nodes could have cyber direct, indirect or inter dependences with local and/or external essential services.

To exemplify this point, the aviation system (airplanes, airports, control towers, etc.) is considered as CI in the United States, Italy, Germany and England; then, services like meteorological monitoring and air navigation are also considered CII services, because their core activities depend exclusively on the ICT [15].

3.3 Cascading failure

Some studies have demonstrated the catastrophic effects recursively that can cause interconnected infrastructures, where the failure of one service may cause disruption in other services [44][33]. Even if the probability of occurrence is low, the result of this may be devastating to multiples services, and may cause a cascade of systems failures [45]; this was based on the study conducted by Havlin in Italy, who explained that an initial failure in an electricity generating plant can cause cascading effects in a large network turning it into fragmented networks [33]. One such example is Colombia. In Colombia there are more than 80 electrical substation plants throughout the country, and these are interconnected with each other, the following figure illustrates an imaginary cascade of failures on some nodes called “D”, which are dependent on its predecessor.

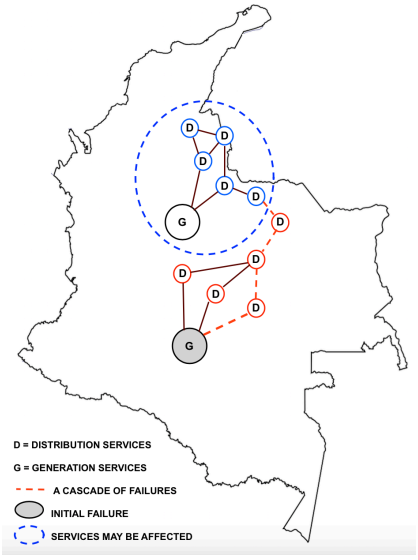

Figure 4. Illustration of a cascading failure, the case of Colombia.

3.4 Cyber dependence

The dependence is understood as a connection among infrastructures, where one service is directly correlated to the state or for the generation of the other services [1][17][18]. The cyber dependence may help to identify services as critical because their connections can demonstrate that one service in whatever kind of relationship such as direct, indirect or interdependence may cause disruption or failures on others by its cascading effects [7].

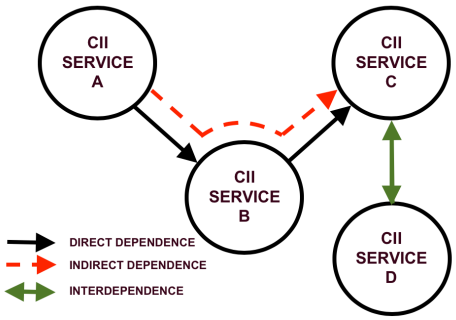

Figure 5. Example of types of relationship among CII services.

As is shown in the figure above, the function of the node "C" depend directly on the function of node "B"; as well, indirectly on the function of the node "A"; and, it has a mutual relationship with node "D". Then, a cyber attack against node "A" could cause a disruption on the other three nodes.

In Europe, dependence are classified in two levels [7][23]:

1) National dependencies: this level includes intra-sector and cross-sector, it means that CII services that belong to specific CI sector can have a strong relationship among other essential services in the same sector (intra-sector), and/or among CI sectors, called cross-sector. One example is the influences that have the electricity and ICT on others other CI sectors;
2) Cross-border dependencies: In 2015, the CCDCOE released a research paper in which clarified that disruption of an essential service outside the country can cause major damage to essential services within the country and vice versa, also the cascading effect can be extended to other countries, because of their cyber dependence and not the land borders [23].

To conclude, cyber interdependence could be defined as the relationship between CII services, where the states of them depend on the storing/processing/exchange of electronic data along network links. As shown below:

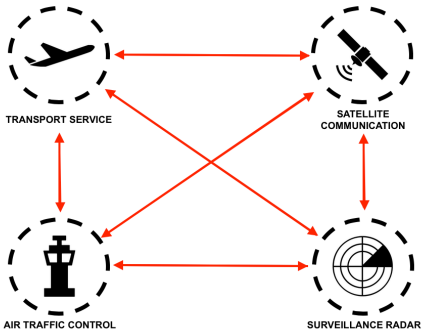

Figure 6. Illustration of cyber interdependencies between some CII services.

4 Generic Criticality Criteria for a Quick-Prioritize

Information and communication technology (ICT) constitutes one of the most important elements of the CII services [4]. This element includes concepts such as vulnerability, threat and consequence that can be used to calculate the impact of ICT's disruption [12][35]. As was clarified in the background chapter, many infrastructures are of importance, but can become critical factors when their disruption can significantly affect people's lives, economy, etc., in other words, criticality is used to assess the impact level of essential services in countries if it suffers a disruption, by using the combination of two influences [12]:

1) Importance: In the CII's context is denoted the relevance of a service for a great percentage of society;
2) Risk: It occurs when the service becomes a threat to the environment, i.e. by not provide water to the population anymore.

According to the researchers the most common approach to catalogue an infrastructure as critical is through the use of comprehensive criticality criteria [7][12]. In fact, Estonia proposes seven criteria for the identification of their vital services[15]; these are:

1) Number of benefit users;
2) Frequency of use;
3) Replacement timeframe;
4) Dependence;
5) Number of services with the same characteristics;
6) Purpose;
7) Timeframe of perceiving the consequences; and, influence on the life.

However, the full protection of a service against cyber attacks is not possible, nor is it possible to prevent the cascading effect that once in flow is very difficult to stop [2]. Because of that, countries include dependence as criteria. The service itself is not only representative of a criticality for society, but also when that supports other essential services; the service in and of it could become critical. The table No. 3 shows a list of minimum criticality criteria used by some countries during the CI assessment.

Table 3. Criteria established by some countries.

Impact Criteria	Country
Public effect (number of population affected); Environmental effect; Economic effect; Political effects; Psychological effects; and, Public health consequences.	The European Commission[16] (Directive of the Council, 2006)
Public health and safety; economic; psychological; and, governance/mission impacts.	The United States[17] (National Infrastructure Protection Plan, 2009)

[15] Retrieved by personal interview (2016, March 8). Interviewer Code: ID_3
[16] The European Commission. (2006). Viewed on 10-Feb-16. Retrieved from http://goo.gl/wqNc3w
[17] National Infrastructure Protection Plan. (2009). The United States. Viewed on 10-Feb-16. Retrieved from https://goo.gl/4oOb6a

Although each country defines its own criteria, most of them have similar applicability so as to determine what to identify as critical [12]. This in turn allows a prioritization of the table of protection in order to allocate financial resources and efforts.

4.1 Analysing qualitative interviews

To understand the vision, interpret an overview and draw from the expertise of professionals on CII is one option for collecting new insights for the identification of generic criticality criteria [46]. The 17 people interviewed during this research represent the specialists and holders of expert knowledge in CII; actually, this was performed and distributed throughout 4 kinds of areas, the interviews were carried out by face-to-face (7 of 15); skype* (8 of 15); telephone** (1 of 15); and, email*** (1 of 15). As shown in the following table:

Table 4. List of interviewees (CO=Colombia; EE=Estonia; and, DE=Germany).

Cod.	Office Interviewed	Academic	Public Policy	Technical	Other
IN_1	The Organization of American States *				X
IN_2	Kaspersky Lab *			X	
IN_3	Ministry of Interior (EE)		X		
IN_4	AVIANCA airline (CO) **				X
IN_5	Tallinn University of Technology	X			
IN_6	Tallinn University of Technology	X			
IN_7	University of Andes (CO) *	X			
IN_8	University of Andes (CO) ***	X			
IN_9	EE-CERT			X	
IN_10	EE-CERT			X	
IN_11	CO-CERT *			X	
IN_12	LV-CERT *			X	
IN_13	CCDCOE (EE)				X
IN_14	CCDCOE (DE)				X
IN_15	Direction of Public Safety and Infrastructure (CO) *		X		
IN_16	The National Department of Planning (CO)*		X		
IN_17	The National Department of Planning (CO)*		X		

Most interviewees agreed the importance of assessing CII services to establish protection priorities, because governments can then allocate financial and technical resources, the interviewees responded to the question as follows:

What criteria will you use to identify Critical Information Infrastructure services?

Table 5. List of interviewees (I1=Interviewer 1; and, I2=Interviewer 2).

Code	Office Interviewed	Economy Property	Health and Safety	Cyber Dependence	Others
IN_1	The Organization of American States	X	X		
IN_2	Kaspersky Lab	X	X	X	
IN_3	Ministry of the Interior		X	X	X
IN_4	AVIANCA airline	X	X		
IN_5	Tallinn University of Technology – I1	X	X		
IN_6	Tallinn University of Technology – I2	X	X	X	X
IN_7	University of Andes - I1	X	X		
IN_8	University of Andes - I2	X	X		
IN_9	EE-CERT – I1	X	X		X
IN_10	EE-CERT – I2		X		
IN_11	CO-CERT	X	X	X	
IN_12	LV-CERT	X	X		
IN_13	CCDCOE – I1	X	X	X	
IN_14	CCDCOE – I2	X	X	X	X
IN_15	Direction of Public Safety and Infrastructure	X	X	X	
IN_16	The National Department of Planning – I1	X	X		
IN_17	The National Department of Planning – I2	X	X		X

As a result of the analysis by semi-structured qualitative interviews and due to the respondents belonging to organizations involved in academic researches, monitoring or identifying essential services in countries, such as: Latvia, Estonia, Colombia and Germany; the following criteria were mentioned to prioritize essential services, as shown below:

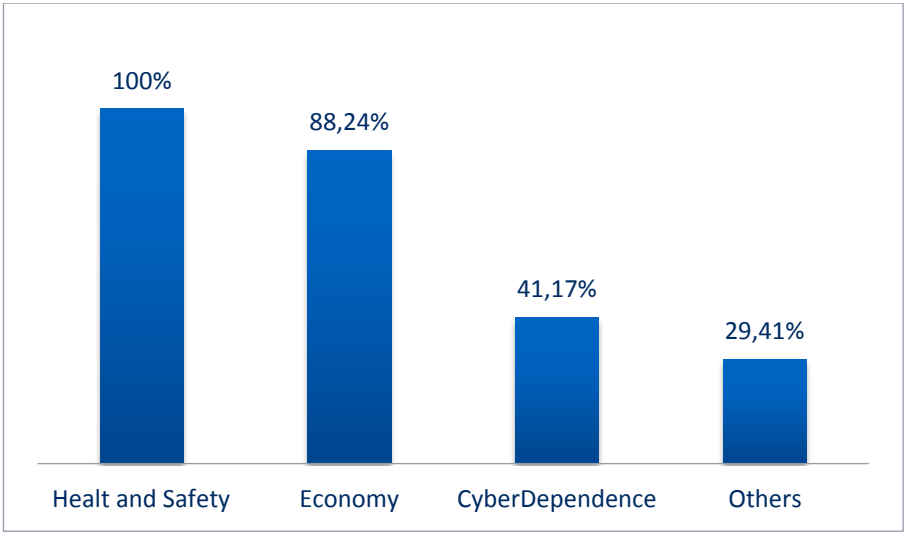

Figure 7. Primary statistical data gathered from interviews.

The table above illustrates that 100% of the interviewees considered the impact of health and safety as the most important criteria for the prioritization of essential services in any country. This was followed by 88.24% of the interviewees, believing the economy played a meaningful role, and 41,17% of interviewees cited that cyber dependence could affect other essential services.

Those criteria offers by interviewers could be combined with other criteria defined by countries such as: The United States and the European Union Members, whom have already identified their essential services. Even though, the final list may be influenced by political decisions, priorities, responsibilities and characteristic specific to each nation, this chapter proposes an adaptable matrix with a list of generic criticality criteria and factors, which are described in the next step.

4.2 List of criteria for evaluating of CII services

In supporting criteria offered by interviewers and with information from countries belonging to the European Union, and The United States, the following table shows criteria that are similar and could be included in a generic list of criticality criteria.

Table 6. Comparative list of criticality criteria.

Impact criteria	The European Commission	The United States	Interviewers
Economic	X	X	X
Environment	X		
Public health and safety	X	X	X
Political/Governance	X	X	
Dependence			X
Psychological	X	X	

Although, the European Commission established their criteria in 2006 and The United States in 2009, in recent years new concepts related to CII have appeared, cyber dependence being one such concept (cross-sector and cross-border). To be as precise as possible, in 2015 the CCDCOE released the regulating cross-border dependencies of CII, in which it was demonstrated that very few countries consider dependence as a criteria; the

document also described almost all CII services of all countries are interconnected and that a disruption could affect other essential services; indeed, these criteria could have a trans boundary impact in neighbouring countries [29]. Then, based on some research papers and the vision and overview from the expertise of professionals on CII, this research has chosen to include cyber dependence as a criterion in order to offer an adjustable and updated matrix. Therefore, the following list is taken as generic criticality criteria in this work.

1) Public health and safety impact;
2) Economy impact;
3) Psychological impact;
4) Political/Governance impact;
5) Dependence impact.

In order to establish a common procedure, the impacts are evaluated with respect three factors [35][12]:

1) Effects of time;
2) Magnitude;
3) Scope distribution.

This list is designed in adaptable way, in order for stakeholders to add or delete a criterion vertically and/or a factor in order horizontal accordingly; thus it will not suffer changes in its procedure, because the calculation works as a matrix. Where the final result of that matrix would represent the position of each CII service in the table of protection priority.

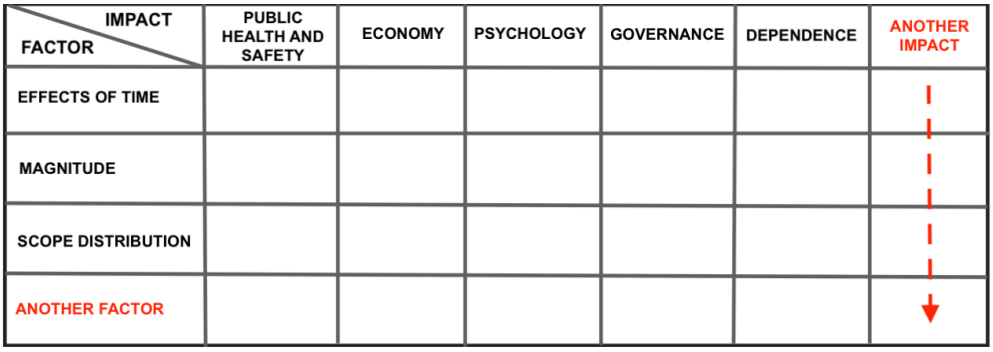

Figure 8. The adaptable matrix of criteria for evaluating CII services.

All CII services listed should be evaluated as illustrated below. Nevertheless, each range of time, level of gravity and scope distribution can adapt their percentages or proportions depending on national needs and characteristics that each country is unique and thus its needs are not equal.

First, the effect of time: it is represented in hours, which is the point that the loss of an element could have a grave impact on society. For example the impact an attack against the food distribution service could be reflected on society after some days or weeks, which could subsequently lead to food shortages in a given population. This factor is illustrated as:

Table 7. Effect of time in hours.

Range in hours	**More than 60**	**48 to 60**	**36 and 48**	**24 and 36**	**0 and 24**
Value	1	2	3	4	5

Second, the effect of magnitude is caused by the interruption of a particular CII service that can be estimated by using the following risk assessment matrix (Table No. 8), which was modified from Department of Defence Standard Practice of United States [47]. In addition, the description and range of values of severity categories (Catastrophic, Critical, Marginal and Negligible) and probability levels (Frequent, Probable, Occasional, Remote, Improbable) can be found in the official web site[18].

Table 8. Magnitude or level of impact took from MIL-STD-882E.

	Frequent	**Probable**	**Occasional**	**Remote**	**Improbable**
Catastrophic	5	5	5	4	3
Critical	5	5	4	3	3
Marginal	4	4	3	3	3
Negligible	3	3	2	2	1

Third, scope distribution is the value that can be obtained by evaluating how a proportion of the population can be affected with respect to a service if it suffers a cyber attack. As shown below:

Table 9. Population of people affected.

Percentage/amount of population affected	**Value**
More than {insert maximum value}	5
In the range of {insert value}	4
In the range of {insert value}	3
In the range of {insert value}	2
In the range of {insert minimum value}	1

Then, the value per each criterion is calculated by a mathematical operation called as Rn, where n is the number that represents each column, as shown below:

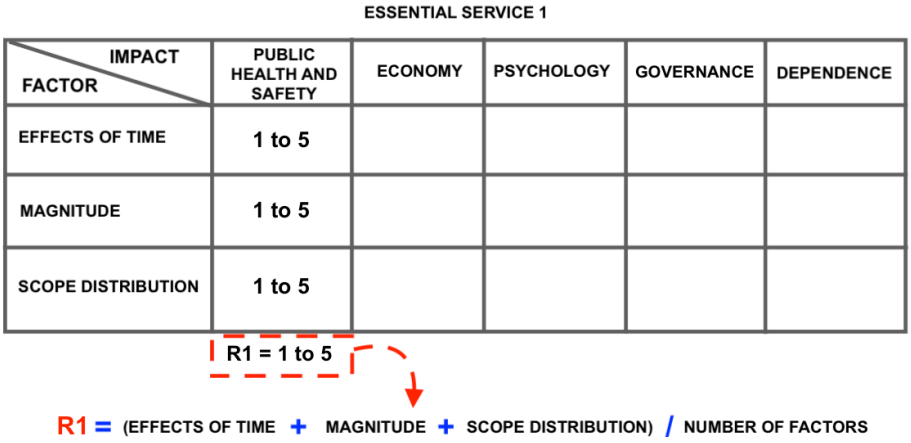

Figure 9. Illustration for the evaluation of each criterion.

[18] Department of Defense Standard Practice. (2012). System Safety. The United States of America. Viewed on 12-Mar-16. Retrieved from http://goo.gl/2rgU48

Therefore, criticality ranking is estimated by a formula, this allows prioritizing each criterion that is represented by acronym "P" and "R" symbolises the result that was calculated in the previous figure, which represents the sum of the factors divided into the total number of them.

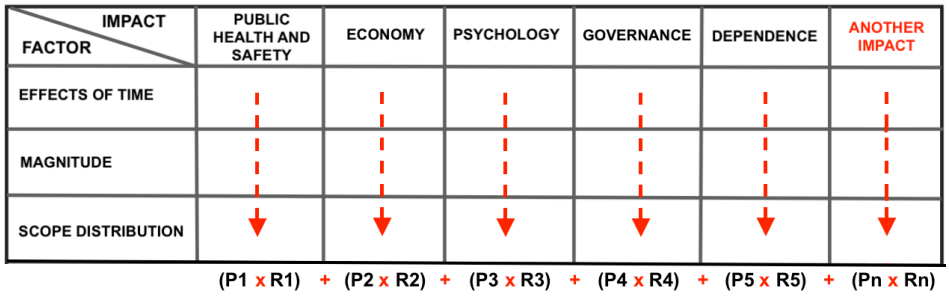

Figure 10. Calculating process of all subsets.

Next, to calculate the value of the sum of all subsets from (P1 x R1) to (Pn x Rn), where n represents the last number of the criteria; the following imaginary example could help understanding a deeper this procedure. For the country X, the priority is to mitigate the public health and safety impact, which symbolizes their nation's characteristics. Therefore, to P1 will have assigned the highest value, which could be the total number of criteria, i.e. P1 = 5; and the other values will be assigned in descending order to other criticality criteria depending their importance. As illustrated below:

1) Public health and safety impact; P1=5
2) Economy impact; P2=2
3) Psychological impact; P3=3
4) Political/Governance impact; P4=1
5) Dependence impact. P5=4

In addition, if a country has two or more criterion with the same importance, these can have the same value of impact (I.e. P1 = P5 = Pn) for all of them.

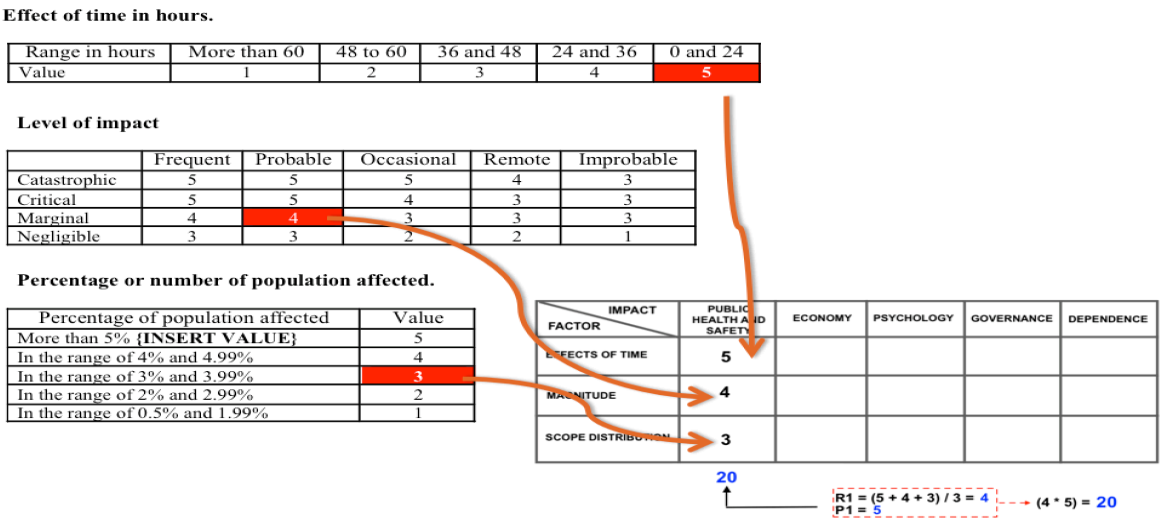

Figure 11. Illustrating process to calculate the value per criterion.

As a result, the sum of all subsets indicates that the highest number will be the first CII service in the table of protection priorities. Other essential services and corresponding values are organized in descending order, leaving till last the smallest value. Moreover, the

multiplication inside of each subset (Pn x Rn) can help reducing the impact of a possible human error during data entry in the matrix because each subset is multiplied independently, as shown in fig.12; mitigating the rest of the formula suffers a strong influence.

Subsequently regarding static testing, it became apparent that the final result could vary in the range of ±6.67 points in the table of national protection priorities depending on the value assigned to prioritizing each criterion "Pn". To illustrate this point, assuming that if all fields of an adaptable matrix is filled with a value of 5, and the values of P1 to P5 are assigned in descending order as follows P1=5, P2=4, P3=3, P2=2, and P5=1; the final result will be 75 points. Otherwise, if a possible human error during data entry changed one of the public health impact's values by 1 instead of 5, the result (the sum of all subsets) will be changed to 68.3 (6.67 points less than the first value calculated).

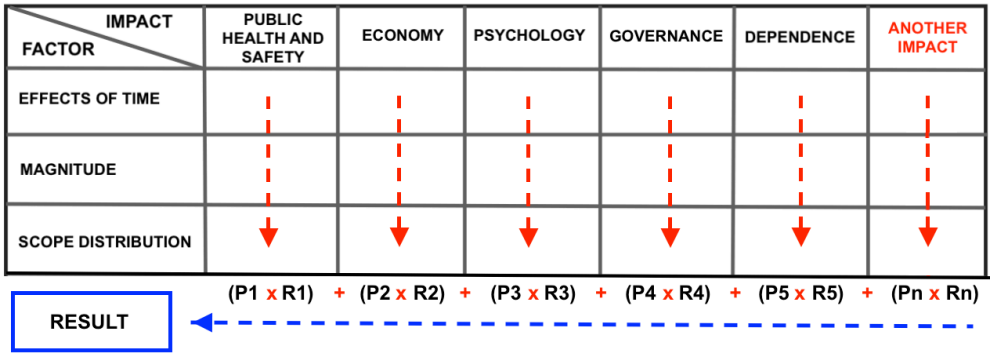

Figure 12. Calculating process of criticality ranking for CII services.

5 An Illustrative Framework for Identifying CII services

The identification of Critical Information Infrastructure (CII) services depends on the ability of, and a good understanding between, public and private operators [48]. Therefore, the aim of this chapter is to propose an illustrative framework called as 360-DEGREE-FEEDBACK that describes the flow of information among national decision makers, CII operators and collaborating institutions in order to identify of CII services based on eight steps, as seen in fig.13, these are:

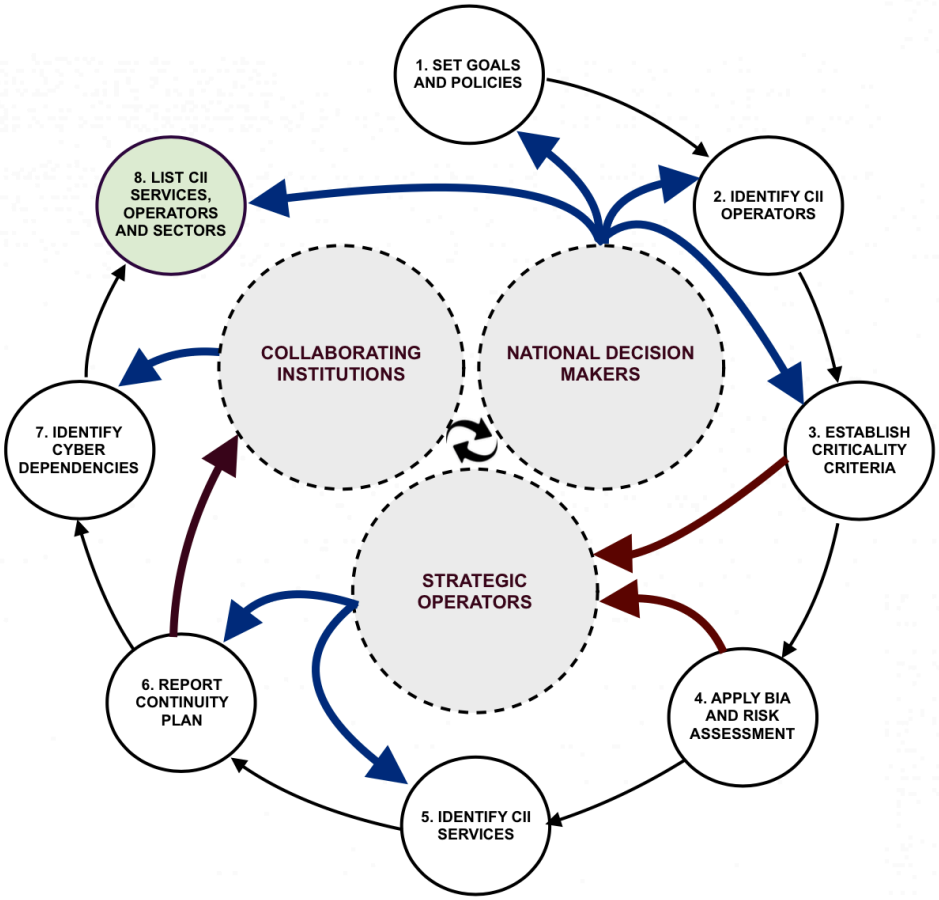

Figure 13. 360-DEGREE-FEEDBACK framework for the identification of services.

The 360-DEGREE-FEEDBACK follows a step by step framework of the principal tasks carried out for identification of services, and on-going interaction among the main stakeholders; in order to keep a continues communication that allows exchanging information and resources.

5.1 Set goals and policies

National decision makers are responsible for establishing the goals and policies for the identification and protection of national CII services not only because the government is solely responsible for establishing guidelines and to protect economic national security, but also as it holds a duty of care for the safe functioning and operation of which, affects all areas of citizens' life.

Then, to reach a comprehensive list of protection priorities of CII services, the goals and policies must be focussed on national interests, which are described in detail as: a set of achievable objectives, stakeholders involved, time and financial resources, during all

process of the identification of CII services. This step can give clarity to other steps, it allows for the visualization of scenarios, allocation of resources adequately and efforts' rationalization.

5.2 Identify CII operators

The principal mission in this step is to display a list of CII operators instead of essential services. Therefore, this research proposes that potential public and private providers (CII operators) can be selected through the analysis of different factors, these are:

1) The geographic area that could be affected;
2) Operating income;
3) Number of benefit users;
4) Loss of human lives.

This kind of information is highly important for any country because it can show the relationship among people, business services and the economy of the nation. In most cases, the potential CII operators have considerable geographic coverage and their business services influence a significant proportion of the population. For example, in Colombia if a company that offers electricity distribution service is under cyber attack, it not only has cyber dependence with other essential services, but also the energy sector represents 53% of the total operating income in Colombia[19] and a disruption could inevitably affect people's life, such as: hospital care, water distribution, food supply, etc. Therefore, selecting the CII operators based on geographic area, financial data, loss of human lives, and number of benefit users allow to the government to make sure that at least the majority of the essential services can be taken into account regardless of whether a CI sector is considered as critical or not.

5.3 Establish generic criticality criteria

This step establishes a minimum criterion for the identification of decentralized essential services where its possible failures can impact negatively or became intolerable for society [12]. As shown in the previous chapter the criticality criteria could be calculated with the correct and available information, the generic criticality criteria establishes in this work are:

Generic criticality criteria:

1) Public health and safety impact;
2) Economy impact;
3) Psychological impact;
4) Political/Governance impact;
5) Dependence impact.

Factors:

1) Effects of time;
2) Magnitude;
3) Scope distribution.

Nevertheless, as is described in the Chapter 3: Generic Criticality Criteria for a Quick-Prioritize; this list is designed in adjustable way, in order for stakeholders to adapt a criterion vertically and/or a factor in order horizontal accordingly; and, each range of time,

[19] Superinterndencia de Sociedades (2015). The largest companies of Colombia. Viewed on 09-Feb-16. Retrieved from http://goo.gl/raExgT

level of gravity and scope distribution can adapt their percentages or proportions depending on national needs.

5.4 Apply a BIA and risks assessment

First of all, infrastructure owners are responsible for identifying their CII services based on suitable methodologies, where the threats, vulnerabilities and consequences of business services are correlated with information technology. One methodology uses a combination of Business Impact Analysis (BIA) and risk assessment, the main task is to identify the principal business services of the organization (importance), as well, as being a potential target from cyber attacks, malware, etc. (risk) [36][38][37].

On the one hand, risk assessment is the result of the intersection of threats, vulnerabilities and consequences associated with an incident by accidental or non-accidental cause [18]. In 2007, professor Herdenson established a formula for the calculation of risk, which is composed as follows [36]: Risk = Threats x vulnerabilities x consequences.

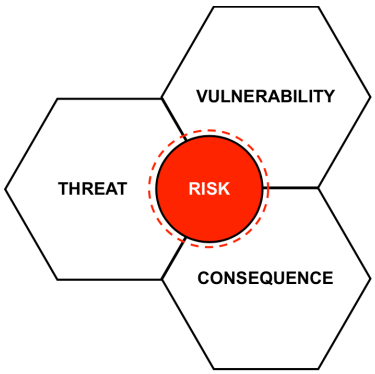

Figure 14. Illustration of crossing among threat, vulnerability and consequences.

Threat represents any person or event with the potential to cause damage in a system [49], then a potential unauthorized access to information of an essential service could be categorized as a threat including timeframe, technique and resources. Vulnerability is any weakness that could be exploited by someone else [49], for example unpatched-software that has access to the information stored in a database. And, consequence is the amount of loss or number of the population affected from a successful cyber attack.

On the other hand, the task of BIA is to identify the essential services and to understand the impact and effect the disruption or failures of these processes have on a company; actually, Business Continuity and Disaster Recovery for IT Professionals book proposes seven steps to perform a formal BIA, such as [37]:

1) Identify principal business processes;
2) Establish requirements for essential service recovery;
3) Determine technical, financial and human resource dependencies;
4) Determine impact on operations;
5) Develop priorities of business processes;
6) Develop recovery time requirements;
7) Calculate operational, legal, and financial impact of disruption.

Therefore, this step includes a combination of the BIA and risks assessment in order to understand more broadly the correlation of the essential business services and potential threats; in fact, the purpose is for operators to estimate the impact of downtime of each essential services and the elements that will be impacted after the failure; as a result of this combination each CII operator is able to establish an effective business continuity plan

that includes an analysis of financial impact and operational impact of any essential business service disruption as a mitigation strategy, which is part of the security and emergency manager plans of the nation [38][37].

5.5 Identify CII services

The increasing reliance of essential services on Information and Communication Technology (ICT) assigns important responsibilities for organizations and governments [15], who have to secure the proper functioning and to reduce the impact or consequences from a cyber attack.

The purpose of this step is to assign the responsibility to each CII operator to describe their services that its core activity depends on ICTs. As is visualized in the previous chapter to reach this mission each CII operator should apply the generic criticality criteria generated by the national decision makers, the essential services can be located in a range of values in order to map the final list of national protection priorities of CII services.

5.6 Report continuity plan

As a result of the combination of the BIA and risk assessment and after the application of criticality criteria to each essential service, CII operators must report the prioritization core business processes, which contain the identification of assets, vulnerabilities and threats, as well as the evaluation of options for recovery; in other words, this plan at a higher level describes the measures to be taken to mitigate and minimize the effects during and after a failure or a significant disruption of an essential service [38][40]. Although, the real elements depend on a government's needs, such as particular hazards, priorities and responsibilities, there is a minimum of elements that a continuity plan includes [35]:

1) Name of essential service;
2) Sector it belongs;
3) Channels of communication in case of a cyber incident;
4) Historical incidents or failures;
5) Recovery time and duration;
6) Linkage among third-party services and technical staff for recovery of an essential service.

5.7 Identify cyber dependencies

Cyber dependence is a relationship among essential services, where one essential service can influence the state of the others[1][17][18]. Therefore cyber dependence may help to identify services as critical because their connections can demonstrate that one service in whatever kind of relationship such as direct, indirect or interdependence may cause disruption or failures on others by its cascading effects [7].

Collaborating institutions such as national CERT, universities and/or organizations devoted to release guidelines and identify CII services could help to correlate this kind of interconnectivity by using two perspectives [7]:

1) Intra-sector dependencies, means that CII services that belong to specific CI sector can have a strong relationship among other essential services in the same sector;
2) Cross-sector dependencies, is the result of an intersection of the interconnectivity among CI sectors, such as: electricity, which has a strong influence on other CI sectors.

The importance of the identification of cyber dependence among essential services and cross-sector industry can aid in understanding and analysing the impact of cascading failures on the CII services as a system. As is illustrated below, the red line exemplifies the probable cyber dependence among services and the blue line represents the strong dependence of society on CII services for their proper functioning.

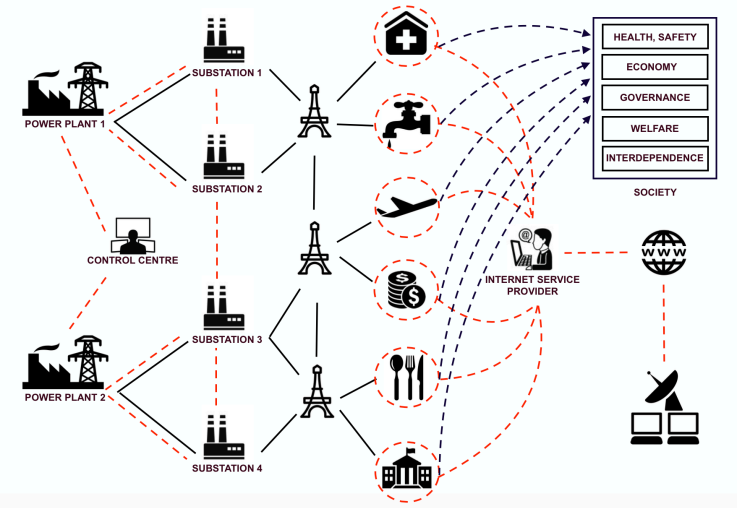

Figure 15. Illustration of potential cyber dependencies between CII services.

5.8 List CI services, operators and sectors

This is the last step of the flow of information between stakeholders, which is based on the final list of essential services enumerated in the table of protection priorities, it recursively could make a list of CII operators involved as well as a list of CI sectors. Indeed, in accordance with Estonia, the importance is to identify and ensure essential services that really should be protected against malware or cyber attack, and illustrate that its failure or disruption could be negatively reflected in society. The following table exemplifies the final list of national protection priorities:

Table 10. List of CII services, operators and sectors sorted by protection priorities.

#	CII service	CII operator	CII sector	Criticality ranking	List of cyber dependencies
1					
2					

Although, the final list of national protection priorities could include a large number of CII services for some countries, it may be influenced by national needs, political decisions, priorities, responsibilities and characteristic specific to each nation. To illustrate this point, if a hospital care or emergency healthcare service that is located at the end of the list suffers a cyber attack, it would likely cause loss of human lives; because of their cyber dependent on ICT. Therefore, in order to have a representative number of CII services according to available human, financial and technical resources, the recommendation in this step is focused on the highest criticality ranking and those potential CII services that could cause loss of human life by a disruption.

6 The Case Study of Colombia

The identification of the national stakeholders, as an accurate terminology for establishing a common understanding of the terms, including the calculating process for criticality ranking that work as an adaptable matrix, and an illustrative framework called as 360-DEGREE-FEEDBACK are the basis to offer an alternative instrument that could be used for collecting relevant information for country as Colombia that have not yet identified their CII services. Therefore, the following case study is based on some secondary statistical information of Colombia; the case's description represents the analysis of behaviour of potential CII services. Nonetheless, this illustration does not pretend to display a real list of Colombia' CII services because the criticality criteria ranking does not belong to the nation' characteristics. On the contrary, this hypothetical scenario is used to exemplify the relationship between two essential services and map the likely position of them in the table of national protection priorities.

To illustrate this point, in 2011 the National Planning Department of Colombia released a policy[20] on cyber security and cyber defence, which contains an analysis of its core problem in that country, and assigning specific policies to regulatory bodies and advisory agencies in CI. In addition, this official document includes a plan of action, which enumerates 33 tasks with their respective stakeholders, cost of implementation and timeframe. Then, countries that want to apply the 360-DEGREE-FEEDBACK framework need to establish achievable goals during all process of the identification of CII services in order to assign specific tasks to stakeholders involved. The following goals are defined in order to exemplify this step:

Goals:

1) Collect and analyse data and documents such as: policies and guidelines released by government, in order to know the priorities and current situation for the identification of nation's CII services;
2) Analyse the largest companies of the country organised in descending order by operating income that allow selecting the potential CII operators;
3) Establish the list of generic criticality criteria with their percentages and proportions per each range of time, levels of gravity and scope distributions based on national interest;
4) Each CII operator should apply its own combination of business impact analysis and risk assessment, and its applicability will be randomly audited by the national CERT;
5) Based on generic criticality criteria established by national decision makers each CII operator will display a list of their essential business services;
6) CII operators should periodically generate a report continuity plan, which will be collected by collaborating institutions;
7) Based on the list of essential services and the continuity plan generated by CII operators, collaborating institutions will analyse the potential cyber intra-sector and cross-sector dependencies and associated cascading effects.

The national decision makers would be responsible for analysing the factors, such as: operating income; the geographic area; loss of human life; and, number of benefit users that could be affected by a disruption. Nevertheless, in order to exemplify and avoid

[20] CONPES document. Op. cit.

disclosure of sensitive information only public financial information would be analysed to select the potential CII operators of Colombia.

According to the World Bank[21], in 2014 the GDP of Colombia was of US $377,7 million. The figures below show the influence of the first 100 companies[22] with the highest operating income in Colombia grouped by sectors. This illustrates that the companies that belong to the energy sector should be taken into account as CII operators; followed by the manufacturing sector and, sequentially by the food, finance and ICT sectors. However, In order to ensure that all essential services are taken into account, this comprehensive instrument considers that in a real scenario a large representative number of companies should be analysed and sorted by operating income, loss of human life, geographic area and the number of benefit users regardless of whether they belong or not to a specific CI sector.

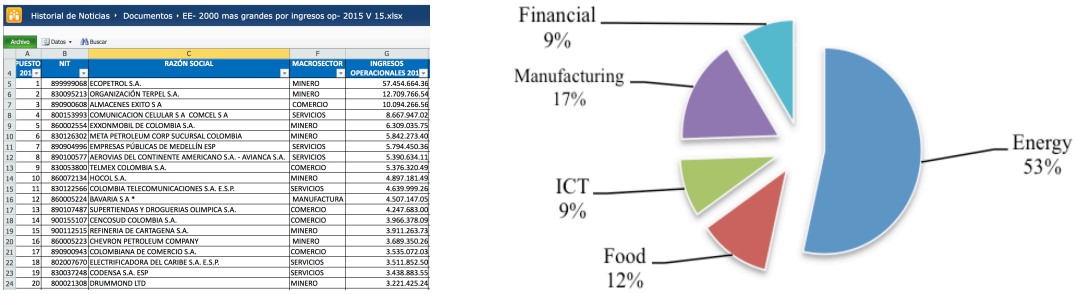

Figure 16. List of the first 100 companies grouped by sectors.

Assuming that the generic criticality criteria proposed in the chapter 4, is considered as an accurate list for Colombia based on its own hazards, characteristics and priorities, which led to political decisions and national decision makers establish these criteria as critical, allowing for prioritization of each criterion that is represented by acronym “Pn” with the values below, as shown:

Criticality criteria:

1) Public health and safety impact. P1=5
2) Economy impact. P2=4
3) Psychological impact. P3=3
4) Political/Governance impact. P4=2
5) Dependence impact. P5=1

Generic factors:

1) Effects of time.
2) Magnitude.
3) Scope distribution.

Actually, to perform a formal BIA it is required as having the right to access specific data of particular CII operator, this information is used to determine the potential effects that can cause an interruption of an essential business service on each area or department [37]. Nevertheless, in order to avoid divulging classified information from any company, this section establishes some tables with imaginary data that could be used for collecting the information in each of the departments of a company based on the seven steps established by professor Snedaker [37], as shown below:

[21] The World Bank. (2016). Data of Colombia. Viewed on 10-Feb-16. Retrieved from http://goo.gl/4srcAO
[22] Superinterndencia de Sociedades. Op. cit.

Table 11. Description of CII services belong to electricity subsector.

Description	
CII services	Distribution, generation, transmission and electricity market
CII operator	CII operator X
CII subsector	Electricity
CII sector	Energy

1) Identify principal business processes:

Table 12. Description of the departments of CII operators.

Department Overview	
Department name	**Distribution department**
Name of BIA respondent	Luis Carlos Herrera
BIA respondent's phone	+37259174418
BIA respondent's e-mail	Carlos.herrera.velasquez@hotmail.com

Table 13. Description of all business processes for each department.

#	Business Process	Description of Business Process
1	Distribution Operations	Transfer of power from regional transmission networks to the home of the end-user, including its connection and measurement.
2	Distribution Commercial	Purchase/sale of electricity on the wholesale market. Transfer of power from/to principal transmission networks to/from other electricity distribution companies.

2). Establish requirements for business service recovery:

Each business process requires defining the system resources used in that process, which its core activity depends on ICT. Recovery Time Object (RTO) represents the time available to restore a system after a disaster, then to get systems back up and running is shown in the table below [37]:

Table 14. List of system resources per business process.

#	Business Process	System Resources	RTO
1	Distribution Operations	PRIME READ	18 hours to recovery
		SCADA	24 hours to recovery

#	Business Process	System Resources	RTO
2	Distribution Commercial	SPARD	18 hours to recovery

3) Determine technical and human resource dependencies:

To estimate this kind of dependency requires access to available, sensitive and accurate data. However, in order to give a tool for displaying this correlated information, the table below could be used:

Table 15. Technical and human resource dependencies.

#	Business Process	Technical Resource (IT) Dependencies	Human Resource Dependencies
1	Distribution Operations	SPARD Distribution application, Databases, routers, switches, PRIME READ application, transmission system, Supervisory Control and Data Acquisition (SCADA), Outage Management System (OMS), ION enterprise.	105 Electricity distribution workers, 2 systems administrator, 1 Database administrator, 1 IT security, 2 specialists in Telecom, and 9 electrical engineers.
2	Distribution Commercial	Remote Terminal Units, Programme Logical Controller, Telemetry system, SPARD Distribution application, Databases, routers, switches, PRIME READ application, transmission system, Supervisory Control and Data Acquisition (SCADA), Outage Management System (OMS), ION enterprise.	8 Electricity distribution workers, 3 assistant, 1 systems administrator, 1 accounting manager, and 3 electrical engineers.

4) Determine impact on operations:

The table below describes the use of the system resources in each business process, which makes it easy to interpret, analyse and calculate the impact of disruption of a particular system resource.

Table 16. Potential impact on operations.

#	Business Process	System Resource	Potential Operation Loss	Provider/OS/Version
1	Distribution Operations	SCADA	A shutdown of three power distribution lines, which would impact 2 of the 23 regions of Colombia, and massive failures in other power plants.	Survalent
2	Distribution Commercial	SPARD	Loss of capacity to sell/buy electricity on the wholesale market.	Energy Computer Systems (ORACLE – UNIX)

5) Develop priorities of business processes:

There are four types of categories for the prioritization of a business service by BIA, these are: critical, vital, important and minor; this means that the CII operators focus the most time on evaluating the critical business services [37] in order to identify their CII services.

Table 17. List of priorities of business processes.

#	Business Process	Priority	System Resources	RTO
1	Distribution Operations	Critical	SCADA	24 hours to recovery
2	Distribution Commercial	Critical	SPARD	18 hours to recovery

6) Develop recovery time requirements:

For accomplishing this section, it requires describing the following terms:

Maximum Tolerable Downtime (MTD) is the result of the following mathematical operation MTD=RTO+WRT, it means that a MTD is the maximum time a business can tolerate the unavailability of a specific business process; therefore, if a business process is classified as critical, it will have a shortest MTD [37].

Work Recovery Time (WRT) refers to the time it takes to get critical business functions back to normal, once the system is re-established, for example: if a system is disrupted by a failure, and the MTD is 72 hours, then 24 hours might be the RTO and 48 hours might be the WRT. Therefore, it means that WTR requires appropriate time to check and ensure that the logs, databases, services, etc., are available after to restore the system; in others words, RTO represents the time available to restore a system after a disaster (to get systems back up and running), and WTR symbolises the time (which is twice as long as RTO) to get critical business back [37], as shown in fig. 17.

Recovery Point Objective (RPO) indicates the amount of data loss that can be tolerated by failure's critical business process, for example: if a CII operator performs real-time data backup weekly, then it could tolerate the loss of a week's worth of information [37].

Then, The following table and figure show the relationship among MTD, WRT and RTO:

Table 18. Illustrating calculation of MTD and RPO.

#	Business Process	MTD	WRT	RTO	RPO
1	Distribution Operations	72 hours	48 hours	24 hours	2 days
2	Distribution Commercial	54 hours	36 hours	18 hours	1 week

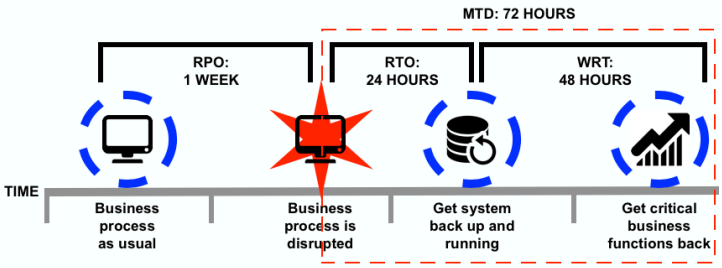

Figure 17. Illustrating calculation of MTD and RPO.

7) Calculate operational, legal, and financial impact of disruption:

The disruption of a business service can cause high operational troubles, because a single incident can not only damage others services on a CII operator, but also the malfunctioning of this would inevitably affecting people's lives and economy of a nation [12]. Then, the business services classified in BIA as critical require significant efforts, such as: human, technical, financial resources in order to get business functions back to normal as soon as possible after they suffer a disruption; as such recovery time is often defined in hours instead of days or weeks [37]. Then, each CII operator should be able to calculate the effects of a disruption of their business services in terms of legal, financial and operational impacts of disruption. To illustrate this point, according to Symantec Corporation report[23], in 2013 the costs of cyber crime in Colombia amounted to COP (Colombian Pesos) 873 million, those malware and cyber attacks affected all sectors, generating consequences on society, such as: unavailable access to information system, the theft of personal identity, loss of information, loss of operational capacity, among them.

On the other hand, once the business impact analysis has been completed, the next step is to assess risks. This can determine the likelihood, potential severity and the number of people (including: employees, customers, users, visitors, etc.) exposed to a particular hazard [37]. Therefore, IT components must be identified individually in order to take into account the potential intra-sector, cross-sector and cross-border dependencies that can be affected. Although, risk assessment is the result of the intersection of threats, vulnerabilities and consequences associated with an incident by accidental or non-accidental cause [18], the risk level could be interpreted as a combination of likelihood (frequency) and impact (severity). Then, once the risk assessment and a BIA have been applied, each CII operator must report to national decision makers the intersection among them, as illustrated below:

Figure 18. Result of calculation of threat, vulnerability and consequences.

Table 19. List of business process and risk identified.

#	Business Process	Risk Identified	Potential Operation Loss	Potential Financial Loss	End-users affected	RTO
1	Distribution Operations	RISK-01 RISK-02	A shutdown of seven electricity distribution lines in Colombia, causing massive failures in other power plants.	USD 2.5 million	1.43 million of customers	24 hours

[23] https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-infographic.es_mx.pdf

#	Business Process	Risk Identified	Potential Operation Loss	Potential Financial Loss	End-users affected	RTO
1	Distribution Commercial	RISK-01	A shutdown of transfer of power from/to principal transmission networks to/from other electricity distribution companies.	USD 4.5 million	3 power distribution lines and 1.43 million of customers	18 hours

Continuing with the hypothetical case that a cyber attack is launched against some electrical substation plants in Colombia, which causes a power cut to a large part of their population, and essential services as electricity distribution is suddenly not available for a substantial period of time. And, in 2014 the total electricity traded in Colombia was 85,390 GWh[24]. Therefore, the next calculating ranking helps to understand protection priorities for CII services:

Table 20. Description of CII operator X, the case of Colombia.

Description	
CII service	Distribution
CII operator	Provider X
CII subsector	Electricity
CII sector	Energy
Total of electrical substations	7 plants
Colombia's population	47,790,000 people (According to the World Bank[25])
Percentage of end-users	3% of the population in Colombia
Total electricity traded by Provider X	2,561 GWh

For calculating the potential public health and safety impact, the following three steps are required:

a) Effects of time: It represents the timeframe of perceiving the consequences on the customers, such as: hospitals, home heating systems, etc. Based on, previous real scenarios, such as: the cyber attack against Ukraine in 2015, which illustrated the cyber dependence of society on electricity and telecommunication; this cyber attack suddenly caused a power cut. And, another case occurred in 2006 when a shutdown of an electricity distribution line in Germany caused massive failures in other power plants located in Italy, France, Netherlands, Belgium, etc., in not more than 6 hours, which affected more than 15 million customers [50]. Therefore, this hypothetical scenario assumes that the timeframe of perceiving the consequences on people into the nation is in the range of 0 to 24 hours.

[24] XM. (2016). Statistical data of electricity distribution. Colombia. Viewed on 10-Feb-16. Retrieved from http://goo.gl/agMEie
[25] The World Bank. Op. cit.

Table 21. Effect of time in hours, the case of Colombia.

Range in hours	More than 60	48 to 60	36 and 48	24 and 36	0 and 24
Value	1	2	3	4	**5**

b) Magnitude: To determine the appropriate probability level requires the application of a security framework as ISO 27001[26], MIL-STD-882E[27], etc. However, in order to illustrate this process the calculation of value will be assumed without real and accurate analysis. Acknowledging that the lights came back on three hours later and workers had to go to substations to close breakers. And, assuming that this probably occurs sometimes (Probable) that there is a significant health impact of 3% of the population in Colombia (Marginal). It is rated as:

Table 22. Level of impact took from MIL-STD-882E, the case of Colombia.

	Frequent	Probable	Occasional	Remote	Improbable
Catastrophic	5	5	5	4	3
Critical	5	5	4	3	3
Marginal	4	**4**	3	3	3
Negligible	3	3	2	2	1

c) Scope distribution: Colombia is home to 47.79 million people. Regarding the cyber attack, which affected an electric utility in 7 of its substations, and killed electricity to 1.43 million of customers, which represents 3% of the total of population in Colombia. It is rated as:

Table 23. Percentage of population affected, the case of Colombia.

Percentage of population affected	Value
More than 5%	5
In the range of 4% and 4.99%	4
In the range of 3% and 3.99%	**3**
In the range of 2% and 2.99%	2
In the range of 0.5% and 1.99%	1

Then, the value per each criterion is calculated by a mathematical operation called as Rn, where n is the number that represents each column, as shown below:

[26] ISMS Auditing Guideline (2008). ISO 27001 Security. Viewed on 20-Mar-16. Retrieved from http://goo.gl/GTI3Ug
[27] Department of Defense Standard Practices. (2012). System Safety. Viewed on 20-Mar-16. Retrieved from http://goo.gl/sLNP3S

IMPACT / FACTOR	PUBLIC HEALTH AND SAFETY	ECONOMY	PSYCHOLOGY	GOVERNANCE	DEPENDENCE
EFFECTS OF TIME	5				
MAGNITUDE	4				
SCOPE DISTRIBUTION	3				

20

R1 = (5 + 4 + 3) / 3 = 4
P1 = 5

(4 * 5) = 20

Figure 19. Calculating sub process of public health and safety impact.

In order to avoid the same process several times with each of the five criteria as done in the previous three steps, the following table is the final result, which was calculated through a static testing and their values was estimated by using real statistics[28] with an imaginary scenario, which aims to map a illustrating final list of national protection priorities of CII services.

IMPACT / FACTOR	PUBLIC HEALTH AND SAFETY	ECONOMY	PSYCHOLOGY	GOVERNANCE	DEPENDENCE
EFFECTS OF TIME	5	3	4	4	4
MAGNITUDE	4	3	3	2	4
SCOPE DISTRIBUTION	3	2	3	2	3

(5 * 4.00) + (4 * 2.67) + (3 * 3.34) + (2 * 2.67) + (1 * 3.67)

49.67

Figure 20. Calculating process for CII operator, the case of Colombia.

The previous step helps to understand protection priorities per each essential service offered by CII operators and improves prediction of failures at a certain decisive moment. Concluding that the final value indicates that the CII operator called as "Provider X" belongs to the national services CII; based on a hypothetical scenario and that CII operator only provides electricity distribution to 3% of the population in Colombia. Even though, this means if someone executes a cyber attack against a CII service, cyber dependence could disturb other essential services, and the malfunction would significantly affect more than 1.43 million people.

Independently and separate from the final result of this case study, it can be shown that CII services become most evident and tangible in the case of a real failure after a cyber attack, when its essential services, such as electricity distribution, are suddenly not available anymore or for a substantial period of time.

Taking another essential services as an example, the aeronautical agency reported that in 2014 aviation industry carried a total of 36,134,568 passengers[29]. In order to continue illustrating this imaginary case, one of the largest airlines in Colombia released some statistical data about their service, these are:

Table 24. Description of CII operator Y, the case of Colombia.

[28] Ministry of ICT, UPME (2014). Data of Colombia. Viewed on 20-Mar-16. Retrieved from http://goo.gl/w3Xzar, http://goo.gl/7q2cRd and http://goo.gl/tXK2fZ

[29] Aeronautical Civil. Op. cit.

Description	
CII service	Airports Operations
CII operator	Provider Y
CII subsector	Aviation
CII sector	Transport
Total airplanes	More than 140 airplanes[30]
Colombia's population	47,790,000 people (According to the World Bank[31])
Total passengers carried in Colombia	46,134,568 passengers
"Provider Y" carried a total of	26,230,000 passengers[32]
Percentage of end-users	56.86% of total passengers in Colombia

This particular case shows that the total passengers carried by "Provider Y" was 56.86% of total passengers; making it a potential CII operator for Colombia, that means if someone executes a cyber attack against Provider Y's airports operations services, this would stop all air traffic, and the malfunction would significantly affect the population in Colombia. In addition, cyber dependence could disturb other vital services as meteorological monitoring, food distribution, emergency and air rescue, etc. As illustrated below:

IMPACT / FACTOR	PUBLIC HEALTH AND SAFETY	ECONOMY	PSYCHOLOGY	GOVERNANCE	DEPENDENCE
EFFECTS OF TIME	5	4	5	4	3
MAGNITUDE	5	5	4	5	3
SCOPE DISTRIBUTION	5	5	5	5	3

(5 * 5.00) + (4 * 4.67) + (3 * 4.67) + (2 * 4.67) + (1 * 3.00)

70

Figure 21. Illustration of calculation of the final value for each CII service.

Furthermore, a report continuity plan at a higher level describes the measures to be taken to mitigate and minimize the effects during and after a failure or a significant disruption of an essential service, it includes certain minimum elements, which are considered as classified information for goverments and organizations. Then, the data must be handled with high levels of protection in order to prevent leakage of information. A continuity plan can be reported by the following tables:

Table 25. Briefly report continuity plan.

[30] Avianca Airline (2016). Our Fleet. Viewed on 22-Mar-16. Retrieved from http://goo.gl/qjo2vs
[31] The World Bank. Op. cit.
[32] Avianca. Operational Statistics. Viewed on 22-Mar-16. Retrieved from http://goo.gl/Paguck

Briefly Report Continuity Plan				
CII operator		Provider X		
CII subsector		Electricity		
CII sector		Energy		
Channels of communication		E-mail, mobile phone.		
Respondent's phone		+37259174418		
Respondent's e-mail		Carlos.herrera.velasquez@hotmail.com		
CII service		Electricity Distribution		
#	Business Process	RTO	Risks	Responsible
1	Distribution Operations	24 hours	RISK-01 / 02	Luis Carlos Herrera
2	Distribution Commercial	18 hours	RISK-01	Juan Camilo Hernandez

In addition, cyber dependence may help to identify services as critical because their connections can demostrate that one CII service may cause disruption on others by its cascading effects [1][17][18]. In order to identify the intra-sector and cross-sector cyber dependencies, the following table can illustrate the likely relationship between potential CII services. This information should be gathered during the implementation of a combination of BIA and risk assessments, and be analysed by collaborating institutions. Due to the detail of this kind of relationship it is to be considered as classified information for governments; this research proposes the following table in order to be used for correlating the interconnectivity between CII services.

The table also illustrates the dependence levels that a stakeholder can define for describing the cyber dependence of one CII service in function of risk in another (H: high, M: medium, and L: low), for example: if airport operations depend on electricity distribution, and electricity distribution has a high risk of disruption, the probability of airport operation disruption is correspondingly higher; because the airport operations has a high dependence (H) on electricity distribution.

CI SECTOR	CII OPERATOR	CII SERVICE	BUSINESS PROCESS	AIR TRAFFIC CONTROL	DISTRIBUTION OPERATIONS	DISTRIBUTION COMMERCIAL
TRANSPORT	PROVIDER Y	AIRPORTS OPERATIONS	AIR TRAFFIC CONTROL		H	
ENERGY	PROVIDER X	ELECTRICITY DISTRIBUTION	DISTRIBUTION OPERATIONS			H
			DISTRIBUTION COMMERCIAL		H	

Figure 22. Illustration of cyber dependencies; H=high, M=medium, and L=low.

As a result, the 360-DEGREE-FEEDBACK framework recursively could present a list of CII services, CII operators involved and CI sectors as well as a list of criticality ranking. Although, only two CII services with real statistical data were analysed in a hypothetical scenario, the national protection priorities would be listed in the order shown below:

Table 26. List of CI services, operators and sectors analysed during the process.

#	**CII Service**	**CII Operator**	**CII Sector**	**End-users affected**	**Criticality Ranking**	**Cyber dependence**
1	Airport operation	Provider Y	Transport	26 million	**70**	Electricity distribution
2	Electricity distribution	Provider X	Energy	1.43 million + 3 electricity distribution companies	**49.67**	…

7 Conclusions

The development of a comprehensive instrument for Identifying Critical Information Infrastructure (CII) services was achieved due to:

1) The identification of main stakeholders, which was hierarchically organised to make it easier to interpret and to avoid unnecessary confusion;
2) A calculating process for criticality ranking that works as an adjustable matrix, where each criterion with its range of time, level of gravity and scope distribution can adapt their percentages or proportions depending on national needs and characteristics to be applied to each country; and,
3) The design of such framework is called 360-DEGREE-FEEDBACK; this describes the flow of information among stakeholders based on eight specific steps.

The above three components are the basis to offer a comprehensive instrument that may be used for collecting information for countries that have not yet identified their CII services as was exemplified in the case study of Colombia. Also where two potential CII services were mapped as illustrated in the table of national protection priorities, ordering the corresponding values of each criticality ranking in descending order, leaving till last the smallest value.

Actually, the identification of CII services has been made possible and is viable because the 360-DEGREE-FEEDBACK framework. The framework follows a step-by-step template of the principal tasks for identification of essential services. On-going interaction among the main stakeholders is key; both stakeholders and the list of tasks were shown to be equally as important as each other and their interaction may lead to work on all levels at the same time, in order to keep a continues communication that allows exchanging information and resources during the process.

In addition, one of the keys to reach this achievement was to extract the CII services from Critical Infrastructure (CI) to be analysed as a whole system; as well as, to describe the importance of society on essential services that its core process depends on Information and Communication Technology (ICT). Indeed, if a cyber attack is carried out against a CII service, it would impact on people's lives, the economy of countries, and its essential services supply because of their cyber dependencies. In fact, cyber dependence not only brings benefits like information sharing or rationalized efforts, but also if a CII service is interrupted the probability of disruptions of other services is potentially very high and may have a cascading effect, which could spread to other countries, due to the nature of their cyber dependence and not the physicality of their land borders.

However, the result of identification of CII services belonging to any country required some additional issues that are not included in this research, such as training of staff, founding of Computer Emergency Response Team (CERT) and creating cross-sector teams to discuss decisions and criteria, among them.

Although, this instrument was not validated due to the need for a real scenario to illustrate the applicability that could consume years or decades for testing and analysing their viability according to population, economy and characteristic of each nation; a separate case of study was conducted using secondary statistical data from Colombia with a hypothetical scenario, in order to illustrate a particular case and offer an exemplifying procedure that could be used for guiding the collection of information to identify those CII services whose core activity relies on ICT.

Therefore, the identification process is the first step to protect CII services against malware or cyber attacks. Consequently, once countries have successfully identified, classified and prioritized its own national CII services, future works could combine this research with new concepts such as cross-border dependencies, which would not only enhance CII services protection within the territory, but also allow for mitigating and mapping the potential cascading effects by disruption of an interconnected service outside of the nation.

8 References

[1] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, Understanding, and Analyzing," pp. 11–25, 2001.

[2] S. V Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[3] S. S. IBM Global Technology Services, "IBM Security Services Cyber Security Intelligence Index," p. 11, 2013.

[4] W. . Zhang, X. Liu, C.-L. Chai, R. Deters, D. Liu, D. Dyachuk, and Z. Baber, "Social network analysis of the vulnerabilities of interdependent critical infrastructures," *Int. J. Crit. infrastructures*, pp. 256–274, 2008.

[5] M. H. A. Klaver and Eric Luiijf, "RECIPE Good Practices Manual for CIP policies," no. July 2011, 2016.

[6] M. Suter, "A Generic National Framework For Critical Information Infrastructure Protection (CIIP)," *Secur. Stud.*, no. August, 2007.

[7] E. U. Agency and I. Security, *Methodologies for the identification of Critical Information Infrastructure assets and services*, no. December. 2014.

[8] E. Nickolov, "Critical information infrastructure protection: Analysis, evaluation and expectations," *Inf. Secur.*, vol. 17, pp. 105–119, 2006.

[9] Organization of American States, "Cyber Security Technical Assistance Mission," 2014.

[10] T. M. Incorporated and N. Klopfenstein, "Report on Cybersecurity and Critical Infrastructure in the Americas," 2015.

[11] T. P. Vartanian, *Secondary data analysis*. Oxford University Press, 2010.

[12] A. Fekete, "Common Criteria for the Assessment of Critical Infrastructures," vol. 2, no. 1, pp. 15–24, 2011.

[13] M. Berndtsson and J. Hansson, "Computer Science and Information Systems Research Projects," ... *Inf. Syst.*, no. 1, pp. 9–15, 2008.

[14] K. Peffers, T. Tuunanen, M. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *J. Manag. Inf. Syst. 24(3), 45-77*, 2007.

[15] S. Zulhuda, "Towards a Secure and Sustainable Critical Information Infrastructure (CII) – A Study on The Policy and Legal Frameworks in Malaysia,".

[16] L. Tabansky, "Critical Infrastructure Protection against Cyber Threats," *Mil. Strateg. Aff.*, vol. 3, no. 2, pp. 61–78, 2011.

[17] J. Laprie, K. Kanoun, and M. Kaâniche, "Modelling Interdependencies between the Electricity and Information Infrastructures 1 Introduction," pp. 1–14.

[18] W. D. Wilde and M. J. Warren, "Visualisation of critical infrastructure failure," *Aust. Inf. Warf. Secur. Conf.*, 2008.

[19] D. Clemente, "Cyber Security and Global Interdependence: What Is Critical?,"

Chatham House, no. February, 2013.

[20] Homeland Security, "What Is Critical Infrastructure?" [Online]. Available: https://www.dhs.gov/what-critical-infrastructure. [Accessed: 10-May-2016].

[21] M. Chertoff, "National infrastructure protection plan," *Dep. Homel. Secur. (DHS), Washington, DC*, p. 175, 2009.

[22] The Council of the European Union, "Council Directive 2008/114/EC," 2008. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114. [Accessed: 10-May-2016].

[23] Republic of Estonia Information System Authority, "Critical Information Infrastructure Protection." [Online]. Available: https://www.ria.ee/en/ciip.html. [Accessed: 12-May-2016].

[24] Federal Office for Information Security, "Recommendations for critical information infrastructure protection," 2016. [Online]. Available: https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html. [Accessed: 10-May-2016].

[25] H. A. M. Luiijf, A. H. Nieuwenhuijs, and M. H. A. Klaver, "Critical infrastructure dependencies 1-0-1," *2008 1st Int. Conf. Infrastruct. Syst. Serv. Build. Networks a Bright. Futur. INFRA 2008*, no. January, 2008.

[26] A. Issa-Salwe, M. Ahmed, K. Aloufi, and M. Kabir, "Strategic Information Systems Alignment: Alignment of IS/IT with Business Strategy," *J. Inf. Process. Syst.*, vol. 6, no. 1, pp. 121–128, 2010.

[27] J. S. Valacich and C. Schneider, "Information systems today: Managing in the digital world," pp. 2–37, 2010.

[28] P. Bocij and D. Chaffey, *Business Information Systems*. 2008.

[29] K. Kaska and L. Trinberg, "Regulating Cross-Border Dependencies of Critical Information Infrastructure," 2015.

[30] L. Montanari and L. Querzoni, "Critical Infrastructure Protection : Threats , Attacks and Countermeasures," no. March, pp. 1–164, 2014.

[31] Government of the Republic of Lithuania, "On the approval of the programme for the development of electronic information security." [Online]. Available: http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf. [Accessed: 15-May-2016].

[32] E. Luiijf, H. H. Burger, and M. H. A. Klaver, "Critical Infrastructure Protection in the Information Age," no. c, pp. 1–10, 2003.

[33] S. Havlin, N. A. M. Araujo, S. V. Buldyrev, C. S. Dias, R. Parshani, G. Paul, and H. E. Stanley, "Catastrophic Cascade of Failures in Interdependent Networks," pp. 1–15, 2010.

[34] S. M. Rinaldi, "Modeling and simulating critical infrastructures and their interdependencies," *37th Annu. Hawaii Int. Conf. Syst. Sci. 2004. Proc.*, vol. 00, no. C, pp. 1–8, 2004.

[35] M. Theoharidou, P. Kotzanikolaou, and D. Gritza-, "Chapter 3 Risk-Based Criticality Analysis," vol. 1, pp. 35–49, 2009.

[36] I. Storkey, "Operational Risk Management and Business Continuity Planning for

Modern State Treasuries."

[37] S. Snedaker, *Business Continuity and Disaster Recovery Planning for IT Professionals*. 2013.

[38] M. Swanson, A. Wohl, L. Pope, T. Grance, J. Hash, and R. Thomas, "Contingency Planning Guide for Information Technology Systems," *Natl. Inst. Stand. techonology*, 2002.

[39] G. Giannopoulos, R. Filippini, and M. Schimmer, *Risk assessment methodologies for Critical Infrastructure Protection . Part I : A state of the art*. 2012.

[40] D. Elliott, E. Swartz, and B. Herbane, *Business Continuity Management 2e: A Crisis Management Approach*. Routledge, 2010.

[41] F. M. of I. Germany, "National Strategy for Critical Infrastructure Protection (CIP Strategy)," no. June, p. 18, 2009.

[42] A. Klimburg, *National Cyber Security: Framework Manual*, no. 1. NATO CCD COE Publication, 2012.

[43] ENISA, "Baseline Capabilities of National / Governmental CERTs Part 2 : Policy Recommendations," *Enisa*, vol. 0, 2012.

[44] O. Yagan, D. Qian, J. Zhang, and D. Cochran, "Optimal Allocation of Interconnecting Links in Cyber-Physical Systems: Interdependence, Cascading Failures, and Robustness," *Parallel Distrib. Syst. IEEE Trans.*, 2012.

[45] P. Kotzanikolaou, M. Theoharidou, and D. Gritzalis, *Cascading Effects of Common-Cause Failures in Critical Infrastructures*. 2013.

[46] J. V Appleton, "Analysing Interview Data," *J. Adv. Nurs.*, vol. 22, no. 13, pp. 993–997, 2008.

[47] Department of Defense Standard Practice, "Mil-Std-882D Standard Practice for System Safety," *Mctechsystems.Com*, no. February 2000, 2012.

[48] NIPP DHS, "Partnering for Critical Infrastructure Security and Resilience. Homeland Security," *Dhs*, pp. 1–57, 2013.

[49] N. O. Bakir, *A Brief Analysis of Threats and Vulnerabilities in the Maritime Domain*. 2007.

[50] D. Bienstock, *Electrical Transmission System Cascades and Vulnerability: An Operations Research Viewpoint*, vol. 22. 2016.

Appendix

I. Semi-structure qualitative interviews

1) How would you define "Critical Information Infrastructure"?
2) What is the relationship between Critical Infrastructure and Critical Information Infrastructure?
3) What set of (technical or otherwise) capabilities must have a CERT for protecting Critical information Infrastructure Services?
4) What criteria will you use to identify Critical Information Infrastructure services?
5) Would you like to add any relevant information to contribute to this research?

II. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Luis Carlos Herrera Velasquez**,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

A Comprehensive Instrument for Identifying Critical Information Infrastructure Services,

(title of thesis)

supervised by Olaf Manuel Maennel and Raimundas Matulevičius

(supervisor's name)

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **25.05.2016**