UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Yuri Andrea Pinto Rojas

Development of National Cyber Security Strategies (NCSSs), and an Application of Perspective to the Colombian Case

Master's Thesis (30 ECTS)

Supervisor: Maria Claudia Solarte Vasquez
Co-Supervisor: Raimundas Matulevicius

Tartu 2016

Development of National Cyber Security Strategies (NCSSs), and an Application of Perspective to the Colombian Case

Abstract:

States around the world face similar cyber-threats that have been addressed in official statements of policy such as National Cyber Security Strategies (NCSSs), towards diverse ends, depending on their capacities, characteristics, ideologies, purposes and/or vision. Generalisations have prevailed resulting in general frameworks and popular practical guidelines that were made to fit the situation of the issuers, commonly from the most developed countries, and departing from assumptions that are not applicable to all of the rest of states in the world. Governments began to realise the times marked a turning point for beginning to think about, and assert, the needs and possibilities of their own countries first, and for issuing more responsive and responsible laws and policies than they have ever had. At the same time, stakeholders recognise that cyber security is a transnational phenomenon that demands global efforts. A smart balance should be reached across levels and sectors to help increase the safe use of cyberspace and unfold its full potential. The general purpose of this work is to conduct conceptual and empirical research with a mixed methodology where the qualitative approach prevails, but also includes a short quantitative exploratory analysis. A comparative analysis of 5 NCSSs, document analysis, a questionnaire administered online and a case study were the methods that resulted in two theoretical contributions: A definition of cyber security, and the formulation of a set of working tools consisting of: the Adaptable and Transferable Guidelines. Both in order to establish the considerations required to complete a process of NCSS development; the suggestions on the Key Performance Indicators self-assessment list that affirms the benefits of measuring parameters; and, the format for essential components to be included in NCSSs. A case study on the Colombian policy formulation follows, and illustrates the applicability of these unbiased guidelines that could help the institutionalization of procedures and standards for more influential public policies and strategies.

Keywords:

Cyber Security, Strategy, Transferability, Adaptability, Guidelines.

CERCS: P170, Computer Science, Numerical Analysis, Systems, Control.

Riiklike Küberturvalisuse Strateegiate (KTS) arendamine ja Kolumbia vaade

Lühikokkuvõte:

Üle maailma seisavad riigid silmitsi sarnaste küberohtudega, millele pööratakse tähelepanu ametlike poliitikadokumentide - küberturvalisuse strateegiate (KTS) - kaudu. KTSid koondavad eri tegevusi, võimekust, kirjeldusi, ideoloogiaid, eesmärke ja/või visioone. Valdavaks on üldistused, mille tulemuseks on üldraamistikud ja populaarsed praktilised suunised, mis on valmis tehtud, et sobida olukordadesse, kus avaldaja neid kasutada saaks. Tihti on antud raamistikud ja suunised pärit enimarenenud riikidest ning tulenevad eeldustest, et need pole kohaldatavad ülejäänud riikidele. Valitsused on hakanud mõistma, et praegu on tegemist pöördepunktiga, kus esikohale tuleb seada siseriiklike vajaduste ja võimaluste loomine ja tõendamine, et seeläbi töötada välja seadused ning poliitikad, mis oleksid võrdluses eelnevatega paremas kooskõlas tegelikkusega ja vastutustundlikumad. Samal ajal tunnistavad sidusrühmad, et küberturvalisuse näol on tegemist riikideülese fenomeniga, mis nõuab ülemailmseid pingutusi. Vaid nutika tasakaaluga erinevatel tasemetel ja sektoriteüleselt on võimalik kasvastada turvalise küberruumi kasutust ja tagada selle potentsiaali täielik rakendamine. Lõputöö üldeesmärgiks on läbi viia kontseptuaalne ja empiiriline uurimus, kus on kasutatud erinevaid metoodikaid. Valdavalt on kasutatud kvalitatiivset lähenemist, kuid lõputöö hõlmab ka lühikest kvantitatiivse uurimise analüüs. Lõputöö valmimisel kasutati järgnevaid meetodeid: võrdlev analüüs viie KTSi osas, dokumentide analüüs, veebiküsitlus ja juhtumikirjeldus. Nende meetodite kasutamise tulemusena formuleerusid töö kaks teoreetilist panust: küberturvalisuse termin ja tööriistakasti sisu. Tööriistakast koosneb suunistest, mis on kohandatavad ja ülekantavad. See loob aluse kaalutlusteks, mis on nõutavad KTSi arendamiseks. Suunised hõlmavad soovitusi peamiste tulemusindikaatorite enesehindamise loeteluks, mis kinnitaks, et mõõdetavatest parameetritest tekib kasu. Samuti on loetletud kohustuslikud osad, mida KTS peaks endas sisaldama. Järgneb Kolumbia poliitikakujunduse juhtumikirjeldus, mis illustreerib erapooletute suuniste kohaldatavust. Antud suunised saaksid olla aluseks protsesside ja standardite ümberkujundamiseks. Selle tulemusena saaks luua mõjusamaid avalikke poliitikaid ja strateegiaid.

Võtmesõnad:

Küberturvalisus, Strateegia, Ülekantavus, Kohaldatavus, Suunised.

CERCS: P170, Arvutiteadus, Arvutusmeetodid, Süsteemid, Juhtimine.

Acknowledgement

My dearest Maria C, I would like to thank you for providing me with unfailing support and guided me to the right direction. I am also grateful to the experts, who were involved in the online questionnaire for this research. Special thanks are given to PhD. Olaf Maennel and PhD. Hayretdin Bahsi, for their valuable comments and recommendations in the begging of this research. Finally, for their encouragement throughout my years of study my deepest gratitude to my family.

List of abbreviations and terms

CI	Critical Infrastructure
ICT	Information and Communication System
NCSS	National Cyber Security Strategy
KPI	Key Performance Indicators
NATO	North Atlantic Treaty Organization
ENISA	European Union Agency for Network and Information Security
OEDC	Organisation for Economic Co-Operation and Development
CONPES-3701	*Consejo Nacional de Política Económica y Social,* National Council on Economic and Social Policy
SME	Small and medium-sized enterprises
DDOS	Distributed Denial-of-Service
ISO	International Organization for Standardization
NSSD	National Strategies for a Sustainable Development
PDCA	Plan-Do-Check-Act
ITU	International Telecommunication Union of the United Nations
UN	United Nations
AG/RES	General Asembly/Resolution
OAS	Organisation of American States
US	The United States
UK	The United Kingdom
NICSS	National Initiative for Cyber Security Careers and Studies
ISACA	Information Systems Audit and Control Association
IT	Information Technology
IIS	Internet Information Services
GPD	Gross Domestic Product
IS	Information System
IoT	Internet of Things
UNP	National Protection Unit
DANE	*Departamento Administrativo Nacional de Estadística,* National Administrative Department of Statistics
ColCERT	*Grupo de Respuesta a Emergencias Cibernéticas de Colombia,* Colombian Computer Emergency Response Team
CCOC	*Comando Conjunto Cibernético*, Cyber Operations Command Joint
CCP	*Centro Cibernetico Policial,* Police Cybernetic Center

EUROPOL	European Union’s Law Enforcement Agency
INTERPOL	International Police
CICTEC	Inter-American Committee against Terrorism (OAS)
CCC	Convention on Cybercrime
GCI	Global Cyber Security Index

Table of Contents

List of Figures

List of Tables

1 Introduction

The purpose of this work is to conduct rigorous conceptual and empirical research. It compares five existing (5) National Cyber Security Strategies (NCSSs), establishes guidelines with adaptable and transferable characteristics, and suggests Key Performance Indicators (KPIs) that governments could observe to develop a sound, durable NCSS, based on needs. The resulting set of tools indicates minimum considerations and state essential components, advocating for the institutionalization of an unbiased standard.

This study used a mixed methodological approach mainly qualitative but also involving a short quantitative exploratory analysis. It conceptualises definitions, approaches and experts' opinions; collected via an online questionnaire for proposing a new meaning and understanding of Cyber Security. It would be of particular help in the improvement of national and international agreements, which are considered vital to improve cyber security at global level. Additionally, the online questionnaire collects information about how the procedural development of NCSSs works in reality its obstacles and procedures. Other methods used for information and data gathering are: comparative interpretative analysis and extensive document analysis.

Nowadays, digitalisation has profoundly affected the way in which society and organisations work, a functional society depends of a set of complex interconnected infrastructures such as energy, telecommunications, transportation and food [1], the majority of these are dependent on digital components. Besides, an increasing number of technological devices populate the world connecting people through optical fibbers, wires and airwaves handling vast amounts of digital information as part of the prevailing lifestyle of into the information age [2].

It can be said that everyday life depends on technologies and governments that must guarantee certain standards of safety and comfort, also to be aware of secure, effective and redundant performance of Critical Infrastructures (CI), digital services and communications. In addition, to protect the digital interests of their citizens, one of the measures that governments take is the development and implementation of public policies; these have to align all government organizations and entities, coordinate all stakeholders, and assign roles and responsibilities rationally [3].

Cyberspace allows for a diverse range of opportunities to communities and individuals: electronic communication, online education, e-government, access to global information, entertainment, etc. But in the same way it exposes people to new threats; "*the more a society depends on ICT, the more it becomes vulnerable to cyber attacks*" [4]. Societies are struggling against diverse sort of attacks that each day becomes more complex. The risk in the cyberspace is always present and new vulnerabilities are detected daily; safety cannot be fully guaranteed when an activity has a digital component.

During the last decade millions of cyber attacks have occurred, an exact number is difficult to calculate because some are not officially disclosed or remain unnoticed by the victims; typologies change and states do not record all necessary statistics. Even when some of them should be considered to cause a high impact, such those targeting CIs or vital services may not be reported. Examples of high impact attacks are: in 2007 Estonian governmental websites were victims of a series of cyber attacks that were politically motivated or the well-known Stuxnet which changes the perception of what could be achieved through the cyber space until the point to be considered as the first cyber warfare weapon [5]. Furthermore, criminals use the cyberspace to do illegal activities taking advantage of the lack of boundaries and global instantaneous reach, the attribution problems related, and the lack of cooperation among the states enables the criminals to be out of reach by law with low possibilities to be convicted or tried for their activities.

Each country has a different set of priorities, aims, vision and interests invested in the cyber security area as a result of the needs, political will, budget, stakeholder's involvement, particular risks and threats, and the country's organisational structure. Those factors significantly influence the development of public policies that have to be tailored to the specific situation. The solution of one country could not generate a template and address the issues of another, even when they appear to share some characteristics.

Societies are in states of constant change; so governmental strategies and policies should be adapted to suit new characteristics as well. States face the challenge of transforming towards new government systems, which must provide effective services, information and knowledge through a variety of technologies [6]. The governments as leaders in the development of National Cyber Security Strategies - NCSSs need proper and efficient solutions, which have to be applicable nationwide.

Cyber security does not matter to states only; the safety of the domains does not only concern strategies, policies, procedures, guidelines or recommendations from the government point of view. The wellbeing and livelihood of the population is also at stake. Also no technical, operational or strategic magical solution exists, especially if focused only on one aspect or issued without input from all sectors affected. This work claims that the need to merge all stakeholders and call in several disciplines arise, coinciding with Chabinisky in that: "*the cyber security challenge can only be addressed effectively by fully understanding the wide range of threat vectors*" [7]. Cyber security so far has just been considered to belong to a technical domain, nested in computer sciences curricula when it regards to fundamental aspects of the social sciences, the humanities and other disciplinary fields. It is at the core of this research to attempt an interdisciplinary task of combining three study areas: Political Sciences, Strategic Management and Information Systems for the development of NCSSs, as Fig. 1 shows.

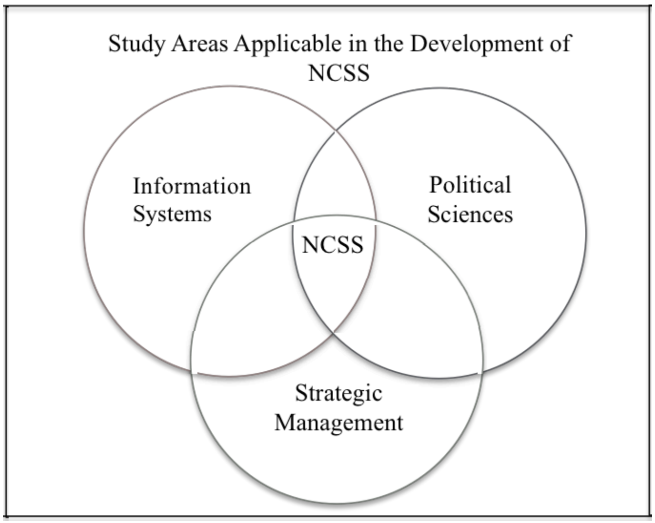

Figure 1. Study Areas Applicable in the Development of NCSS.

While universal solutions that can be applied by all governments are not pursued, a basic set of guidelines and indications on KPIs could be formulated to kept in check a systematic cyber security improvement at national level.

Due to the importance of the NCSSs, the need for proper answers, and efficient solutions, the development of National Cyber Strategies could be said to have become an investigation field. This research proposes a well-thought out and innovative approach of adaptable and transferable guidelines and KPIs, which policymakers could follow in order to improve the development of NCSSs. By adaptable means that may be modified according to differing or new factors, and by transferable that can be used for a variety of countries to their particular characteristics.

To develop an effective and efficient NCSS is the aim of various states; frameworks and guidelines have been published by institutions as NATO, ENISA and OECD, which support stakeholders in the development process but they seems to be specifically geared to developed countries. Despite the guidelines, states do not seem to follow any structure and the development process is not publicly documented. They addressed their NCSS towards different ends depending on their particular realities, characteristics or vision. To the point that currently "*there is no universally accepted explicit definition of what constitutes national cyber security*" [8]. Even, the cyber security meaning differs depending on the sources approaches. At national levels states consider principally up down or a bottom-up approaches, although there are countries, which have not adhered to a formal definition [3].

In order to apply the concept to a real situation, a case study is developed with the Republic of Colombia. The Colombian Government is aware of current and future cyber threats and the need to establish a unified national policy. It released in 2011 the Cyber Security Policy called CONPES-3701 with an implementation time of 5 years. Nevertheless, according to the Organizations of American States, the institutions created by the CONPES-3701 have not reached maturity; resources (financial, time and trained people are lacking) the stakeholder's responsibilities determination is unclear; and, the identification, classification and prioritization of Critical Infrastructure (CI) are missing. In addition to the cyber security policy is out-dated [9].

To address the challenges raised by those recommendations, and to continue the improvement of the Cyber Security status of the country, the development of a new official Cyber Strategy is on the way. The process so far seems to lack methodological validity and would benefit from a more systematic process to improve the cyber security standing of the country. Without a proper background review, the country could make misleading choices that would lead to further inefficiencies and eventually shortcomings. Unfortunately, it could also be the situation of many other countries that cannot find a cyber-security strategy that fits their common and yet basic characteristics.

The research questions that arose to be address the research problem stated were:

- RQ1: What are adaptable and transferable guidelines for developing National Cyber Security Strategies?
- RQ2: How to apply these theoretical perspectives to the Colombian case?

This work is accomplished through the development of the following research tasks, for the first research question (RQ1):

- To analyse the current understanding of cyber security;
- To explore different perspectives on the formulation of NCSS;
- To map/identify the different aspects that are linked to the problem (Infrastructure itself or secured infrastructure, The balance between National Security and data protection, Awareness or/and training and Cybercrime);
- To determine (propose) key performance indicators considering the stakeholders,

principles and objectives, and vision via methodologies such as document analysis and an online questionnaire;
- To establish what could be new transferable and adaptable components of the NCSS.

To complete the work on the second research question (RQ2) the tasks are:

- To investigate the current cyber security status and institutional needs in Colombia, taking a stock of the existing policies, regulations and capabilities;
- To use the case study method to apply the developed guidelines to this concrete case.

The thesis is divided into four chapters: the first constitutes the theory to support this research and presents the theoretical assumptions that the rest upholds. The second conceptualizes cyber security. The third, contains the NCSSs' comparative analysis, proposes the guidelines, the KPIs and the minimum components of a NCSS. The last chapter the conceptual contributions are illustrated with an application to a case study that explores the cyber security situation of the Republic of Colombia. To end, the thesis presents its conclusions and limitations.

2 Background

This chapter reviews the academic standing of the disciplines that are found to overlap in the development of NCSS, as well as the reported factors that policymakers frequently face during the development process. In addition, it discusses, the concept of cyber security and the importance of national strategies in the cyber security field, the guidelines and frameworks developed by researchers and international organizations for the development of NCSS.

On one hand the information systems from Information Systems "*is concerned with the interaction between social and technological issues*" [10]. On the other hand, Strategy from Political Sciences described as the major programs of actions to reach the goals and objectives of the organization and the resource allocation used to relate the organization to its environment [11]. Finally, Strategy Management defined as a procedure to determine the relationship between the organisation and its environment through the use of selected objectives and resources allocation, which allow the development of efficient and effective action programs by the organisation [12]. This interdisciplinary integration allows the bringing about of all necessary support for developing a strategy in cyber security field, which nowadays is found to require more than technical solutions to enhance cyberspace's safety.

2.1 Cyber Security Definitions

Cyber Security has been defined in various ways according to each country needs, perspective, knowledge and vision. The lack of a harmonised cyber security concept around states could cause problems when states need to coordinate, cooperate or collaborate, as they should at least depart from some common grounds. Even, some states avoid defining directly the concept itself, although they develop and implement a specific strategy in this area [3]. It is could be considered an issue when we are talking about protecting a domain, which oversteps conventional borders and demands coordination, cooperation and collaboration among the stakeholders.

National and international organizations as well as researchers have also built definitions according to their needs, backgrounds their perspectives and aims. Some of them define cyber security with an emphasis on information security properties; confidentiality, availability and integrity such as ISO 27000 whereas others focus on combating the cyber threats. To illustrate its point the Table 1, compiles some examples.

Table 1. Cyber Security Definitions.

Source	Document	Definition
Jamaica (Developing Country)	National Cyber Security Strategy of Jamaica (2015). Policy Document.	"*The implementation of measures to protect ICT infrastructure including critical infrastructure from intrusion, unauthorized access and includes the adoption of policies, protocols and good practices to better govern the use of cyberspace.*"[13]

The Netherlands (Developed country)	National Cyber Security Strategy 2 - From Awareness to Capability of The Netherlands (2013). Policy Document.	"*Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred*" [14].
Governmental Definition	Australian Government-Attorney General's Department. Doctrine.	"*Cyber security is one of Australia's national security priorities—Australia's national security, economic prosperity and social wellbeing rely on the availability, integrity and confidentiality of a range of information and communications technology.*"[15]
Academic Research	Paper: Cyber security Policy as If Ordinary Citizens Mattered: The Case for Public Participation in Cyber Policy Making (2012). Doctrine.	"*The body of technologies, processes and practices designed to protect networks, computers, programs and data (and the critical infrastructures on which they rely) from attack, damage or unauthorized access."*[16]
International Organizations	The definition of cyber security by International Telecommunication Union (ITU)[1]. Doctrine.	"*Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets"*[17].
NCSS of Colombia	CONPES-3701 of Colombia (2011)[2]. Policy Document.	*"The state's capacity to minimize the level of exposure of its citizens to cyber threats or incidents."* [18]

2.2 Factors that Influence the Development of NCSSs

The particular characteristics of each country affect the development of public policies; the political will, stakeholder's interests and economic priorities or available resources, are factors that determine the way states develop their policies.

State defence in cyberspace is a current and widespread concern. Although some years ago cyberspace´s militarization was not considered an actual threat, some cases have demonstrated that it is not unlikely to occur. First, in 2007 the well-known Estonian's case in which the country was victim of DDoS attacks and web defacements. Second, in the 2008 Russia was accused of launching DDoS attacks against Georgian websites. A further

[1] ITU is the United Nations specialized agency for information and communication technologies – ICTs. [Available at: http://www.itu.int/en/Pages/default.aspx, viewed on 01 May 2016].

[2] CONPES: Consejo Nacional de Política Económica y Social (Spanish) - National Council on Economic and Social Policy [Available at: https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx#googtrans/gl/en, viewed on 01 May 2016].

instance is Stunext in 2010, which caused physical damage across international frontiers to an Iranian nuclear enrichment plant [19]. The previous instances as proof that the need for national defence in cyberspace is actual not theoretical as it was considered earlier.

Public policy and the political will are vast topics and the latter is in constant change, linked to a multitude of factors that could describe the situation of each country. The political effect over the NCSS is notorious given that at the end, governments classify and prioritize the resources and choose the international policies they want to support or follow. In this context, the government's role is one of initiative and leadership, to motivate stakeholders' participation and to aim at a joint national vision in the development of its NCSS. Mummert & Mummert stated that "*The ideal mixture of leadership and participation always depends on the respective national context*" [20].

ICT also gives to the citizens the possibility to control and intervene in the political management of a country to some extent, social networks and online information have been converted in means to report unconformities or support government strategies. These are source of a heated discussion about the freedom speech and political control, an example of this was the decision in January 2011 to cut off the Internet access in Egypt with the goal of deterring political and social crisis and avoiding external intrusions. Essentially, commented Zhuo, Wellman & Yu, "*The interaction of organized groups, networks, and social media was crystallized in the Egyptian revolt*" [21]. Further instance is the authoritarian Chinese regimen, it restricts the Internet access, filtering content and monitoring online behaviour inside its territory through what were called reactive and proactive strategies by Kalathil & Boas [22].

States must collaborate and cooperate with other countries and diverse organizations for prosecuting responsible of cybercrimes and to improve cyber security level. This is one of the biggest challenges that affront stakeholders due to attribution and jurisdictional issues. Furthermore, there are a variety of cybercrimes that do not exclusively affect companies but society in general. It is important to underline that legislation that contemplate cybercrimes or regulate cybercrime investigation and prosecution schemes has not advanced as fast as technology and communities do. Besides, international cooperation it also affected by internationals affairs of global impact (global warming, refugee crisis, fundamentalism) and independent foreign policies.

Public participation is also essential; this paper argues, in line with Shane, that citizens have to be included in the development of NCSSs. But, on one hand, the awareness of risks and threats related to cyberspace is a common concern of all users and therefore they become first so-to-say gatekeepers, providing a "layer of protection" against threats in this domain. And on the other hand, even the concept of what cyber security represents by itself a challenge "*if people have virtually no understanding of what they are being asked to do or to support"* [16]. Countries that hope to have wider support have to manage citizen's participation problem or the stakeholders' involvement may not happen otherwise. Awareness campaigns and training could be promising tools to progress in this field.

State budgets are normally limited or assigned according to their priorities and that could be far from improving cyber security capacities. Countries in some cases must attend first what is urgent and comply with the basic responsibilities of states: education, food, shelter, a decent health system for the population, etc. Questions on who should pay for what inevitable arise on every matter of national interest including cyber security that governments classify as a national security, but CI's managers, vital services managers, and companies, which are mainly from private sector ask the same: how much is enough to be invested in cyber security and who should run the risks.

To protect national CIs is an important concern when states desire to improve cyber security at national level and stimulate economic growth. Friedman said that "*Governance frameworks must be evaluated in terms of how they promote investment, how they alter incentives, and who will bear the expenses and risks*" [23]. States could offer a wide range of benefits to the managers of CIs to incentivize the function of securing fundamental services. Among these are tax incentives, state loans and subsidies. Another option is to establish minimum cyber security standards by law. NATO has identified some states that support both approaches: incentives and mandates [8].

The relationship between economy and Cyber security becomes narrower every day, states not only contemplate CIs, they also are aware of the small and medium-sized enterprises (SME) such as "*Finance, wholesale and retail trade, transportation, much of manufacturing, and many service industries would slow to a crawl without computers.*" [24]. Additional costs that are difficult to calculate are indirect cost, companies that have dependencies from connected to subsidiaries could be vulnerable through them and benefits of investing in their cyber security cannot be easily measured, as was expressed by Tyler Moore in 2010 "*Systems often fail because the organizations that defend them do not bear the full costs of failure*" [25]. Consequently, SMEs demand governmental support and should be part of the efforts to improve cyber security at national level as at all, their participation should be at different levels and as broad as possible depending on each state. Policy intervention allows seizing the capabilities of private sector, to assign responsibilities among the stakeholders, to reach a minimum cyber security level, to incentivise the productivity and consequently economic growth [8].

Cybercrime's cost is significant as some of the cybercrimes that steal money from consumers are: online identity theft, industrial espionage, critical infrastructure protection and botnets [25]. In 2015, Ponemon Institute [3] did a research about the cost of cybercrime, they found that in the United States the mean annualized cost for 58 benchmarked organizations is $15 million per year as a result of criminal activities related to the cyberspace and increase of 19% in relation with 2014. Germany has the second highest rate followed by Japan. The average cost that a company paid as a negative consequence of cybercrime around the world is $7.7 million. Nevertheless, "*There are no standard methodologies for cost measurement, and study of the frequency of attacks is hindered by the reluctance of organizations to make public their experiences with security breaches.*" [24].

All in all, the need to analyse each case arises, taking into account specific factors that influence it for developing a comprehensive NCSS that address all security concerns in cyberspace and preserve open information and communication networks [26].

2.3 National Strategies and National Cyber Security Strategies

There are 196 countries formally recognised as states, 193 of them are ITU's members and 72 have a National Cyber Security Strategy - NCSS or similar document. According to NATO, there are 63 official cyber strategies and 54 are following ENISA. Europe is the continent where most countries have issued a formal NCSS cyber strategy: 22 out of 28.

Countries such as Belgium, Canada, Estonia, Luxembourg, Austria, Russia, Afghanistan, Malaysia, Ghana, South Africa, Jamaica and Panama have developed and implemented

[3] "*Dr. Larry Ponemon founded Ponemon Institute in 2002. Headquartered in Michigan, it is considered the pre-eminent research center dedicated to privacy, data protection and information security policy".* [Available at: http://www.ponemon.org/about-ponemon, viewed on 01 May 2016].

their NCSS, some of them even released a second version or similar document, it is the case for instance of the United Kingdom, France, the Netherlands, and the United States of America. Luiijf and Besseling indicated that the states address similar threats but each decides to face them in a different way according to their needs, views and aims [3]. On the other hand, recurrent terms have been taken into consideration in the majority of the NCSS such as: Critical Infrastructure Protection, economic prosperity, National Security, cybercrime and awareness. In the CI field some governments decided to face the protection of CI in a separated strategic document as Canada's case that broadcasted an Action Plan for Critical Infrastructures for 2014-2017, although CI's protection is still tied to their NCSS due to the importance that its has to states; CIs control vital services to ensure the normal performance of society, CIs supply water, food and energy, run transportation, telecommunications, health systems and support the banking systems.

Benoit Dupont showed similarities in the content of several national strategies: the desire for better protection of critical infrastructures, the need for national coordination mechanisms, partnerships with private stakeholders as vital assets and the importance of efficient international cooperation [27]. In the same line, Luiijf and Besseling showed connections among 19 NCSS as: to Protect Critical Infrastructure against cyber threats, the requirement for international cooperation, and concerns related to cybercrime. The authors also showed that states called for stakeholders from private sector and public sector to collaborate and cooperate with improving the safeness in cyberspace [3]. A certain tendency is noticed; states their NCSS's from a high perspective towards similar aims and take similar measures, although priorities and visions are different among them.

To analyse if states still have the same similarities or these have changed during the last couple of years towards a new tendency would be the next logical step, but going further even if the states have similar final aims the particular factors of each countries make their policymakers take different ways to the same end, although it does not mean that they can not use a minimum set of transferable and adaptable guidelines, which would help into the development process towards a global objective "cyber security".

How to build an efficient and effective NCSS is a partially responded question. There are a number of approaches for developing Strategies that have been published by different authors. Gaps become evident in the concepts development as; no consensus exists about how strategy-making process should be accomplished in the public sector [28]. Mintzberg identified ten different schools, some of them are prescriptive and others are descriptive such as the entrepreneurial school, the cognitive school, the learning school and the environmental school [29]. More recently, other approaches have been used such as the planning school and National Strategies for a Sustainable Development (NSSD) that was presented as a mix between the formal planning school and the imperialism school, this focused on policy integration, implementation and learning [28]. Furthermore, one of the most popular, created by the private sector, is strategic management defined also as "*the central integrative process that gives the organization a sense of direction and ensures a concerted effort to achieve strategic goals and objectives*" [30].

Discrepancies among NCSS have been detected due to diverse factors, citing Chabinsky: "*no models are perfect for developing strategy, some are at least useful*" [7]. There are not global solutions for helping countries to develop NCSSs that perfectly fit their particular political, economic, cultural, structural and social characteristics. This realisation calls for guidelines that can be matched according to countries needs and interests. The transferability aspect of this proposal would permit its use by different countries around the world.

As interdisciplinary research this work brings the PDCA (Plan-Do-Check-Act) cycle from strategic management domain, known as: the Deming or Shewhart cycle as a basis of the proposal guidelines, although the final phase of it is modified. This cycle demands to focus on the planning phase, which is considered as strength because it is applied exclusively to the development phase without considering the implementation process. In addition, a set of KPIs, initially defined by Kronz as "*measures or metrics that evaluates performance with respect to some objective"*[31], are proposed as an additional tool for measuring the development of NCSS.

2.4 Existing Frameworks or Practical Guidelines for Developing NCSS

Institutions and organizations from private and public sectors have developed a multiplicity of guidelines and frameworks to help in the development of NCSS, a summary of these is presented in the Table 2.

Table 2. Summary of Guidelines and Frameworks for the Development of NCSSs.

Source	Guideline / Frameworks
NATO	National Cyber Security Framework Manual [8].
UN - ITU	National Cyber Security Strategy Guide [32].
OECD	The Digital Security Risk Management for Economic and Social Prosperity by Organisation for Economic Co-Operation and Development [33].
ENISA	National Cyber Security Strategies - Practical Guide on Development and Execution [34].
	Evaluation Framework for National Cyber Security Strategies [35].

The North Atlantic Treaty Organization (NATO) published the National Cyber Security Framework Manual in 2012 to serve *"... as a guide to develop, improve or confirm national policies, laws and regulations, decision- making processes and other aspects relevant to national cyber security*" [8]. Additionally, NATO with collaboration of an experts' group and the University of Cambridge wrote the Tallinn Manual on the International Law Applicable to Cyber Warfare [36] that even tough without focus on the development of NCSSs, contains vital concepts that states should consider when they are elaborating their NCSS, namely state sovereignty, state jurisdiction and state control in the cyberspace added to the traditional state responsibilities. In addition the ITU published the National Cyber Security Strategy Guide mentioning "*issues that countries should consider when elaborating or reviewing national cyber security strategies*" [32].

The European Union Agency for Network and Information Security - ENISA, they developed a guide that is aimed at Member State policy makers interested in managing the relevant cyber security processes within their country called: National Cyber Security Strategies - Practical Guide on Development and Execution [34]. Moreover, they created an Evaluation Framework for National Cyber Security Strategies [35].

One of the most recent documents is the Digital Security Risk Management for Economic and Social Prosperity by the OECD, which was released in 2015. It proposes guidance for a new generation of NCSSs with a focus on managing digital risks and improving the economic and social growth related to the digital world. This document is crucial to the Colombian case, because its government formally launched Colombia's candidacy for this organization in 2013 so the development of the next Cyber Security Policy in the country must be formulated in conformity with this.

Furthermore, Colombia is a member of the Organisation of American States - OAS and as such bound to its guidelines. In 2004 the General Assembly approved the Resolution AG/RES. 2004 (XXXIV-0/04) or The Inter-American Integral Strategy to Combat Threats to Cyber Security, and in 2012, OAS members signed the Declaration on Strengthening Cyber-Security in the Americas.

From the academic point of view Luiijf and Besseling made a good progress analysing and comparing 19 NCSSs and concluding with recommendations on what should be the sections of a NCSS. Nonetheless, they specified that these sections could be changed according to the intended audience and national customs [3]. Supplementary frameworks or guidelines created by private institutions are also available, it is Microsoft's case that released the following document: "Developing a National Strategy for Cyber Security; Foundations for security, Growth and Innovation" [37].

Frameworks and guidelines are available and each state can follow them totally or partially according to their requirements and priorities. Each framework offers a specific focus; in the OECD's case is economic although it considers other factors such as international cooperation and social benefits. The ITU's guidelines concentrate on the choice of the right cyber risks and threats and involvement of all stakeholders.

3 Terminology and Conceptualisation on Cyber Security

This chapter presents the confusion arising from the lack of harmonised terminology in cyber security at national and international levels and describes the advantages of developing common cyber security terminology. It compares various cyber security definitions and analyses the data collected via an online questionnaire. The outcome is a theoretical contribution: a cyber security definition, that countries may consider in their NCSSs.

It can be argued that the transnational cyberspace nature, the increasing of cyber incidents, the escalation of networks use, and the need for national and international agreements claim for a baseline of common definitions to be multilaterally agreed. Countries have expressed their intentions in developing common cyber security terms, such as The United States –US and The United Kingdom - UK that expressed their will to engage in cyber agreements with Russia and China. However, their doctrine addresses towards different cyber security challenges from those the US and UK are concerned with [38].

States cannot establish agreements when they do not agree or adhere to the same connotations of essential terms [39]. Moreover, in the First NCSS of the UK, the urge to develop international principles or 'rules of the road' for behaviour in cyberspace to reduce the risk of escalation and avoid misunderstandings was one of the priorities. Furthermore, a UN group of governmental experts in 2010 recommended elaborating common terms and definitions to General Assembly resolution 64/25. Some efforts to fill the gap were developed by the East West Institute in 2011, which published the "Russia–US Bilateral on Cyber security: Critical Terminology Foundations" with the goal to open a dialogue between the stakeholders from both countries, to understand the position of each other and to set a consensus around the basic definitions of cyber and information security [40]. The second version added 20 new terms in 2014 [39].

There are also a number cyber dictionaries created by diverse organisations as the National Initiative for Cyber Security Careers and Studies (NICSS)[4], and the Compilation of Existing Cyber security and Information Security Related Definitions by the Open Technology Institute New America. Additional samples are: SANS[5] and ISACA[6], that seek to harmonize the terms on cyber security and cyberspace.

The NCSSs are public and official documents in which the national understanding of cyber terms should be reflected. However, there are countries that have not included terminology on their own, such as Spain, Japan and Luxembourg [3].The global nature of cyberspace demands a worldwide cooperation. If states want a better understanding of cyberspace and to establish solid cooperation agreements in this field the first step would be a common baseline of definitions. It would allow an enhancement of the quality of international agreements and cyber diplomacy as well as to aid keeping the peace and creating stability in cyberspace [39].

3.1 Proposal Cyber Security Definition

As a result of the analysis among several Cyber Security definitions that have been published in NCSSs, the experts' opinions and considering the focal points, similitudes and variations, this research proposes the following definition with the aim to harmonise

[4] For additional information look at: https://niccs.us-cert.gov/glossary, viewed on 01 May 2016.
[5] For additional information look at: https://www.sans.org/about/, viewed on 01 May 2016.
[6] For additional information look at: http://www.isaca.org/about-isaca/pages/default.aspx, viewed on 01 May 2016.

the cyber security concepts at national level. It is important to underline that states interests are established depending on each particular case and the application of this concept purports to enlarge cyber security goals towards diverse national vital assess (tangible and intangible) depending on their own priorities, vision and aims:

> ***Cyber security is the set of technical, legal, political, economic, educational, military and/or organisational measures, means and procedures, to protect the interest of the state and the people that conform it, in the cyberspace.***

The non-existence of a broadly acceptable definition that involves multiple dimensions of cyber security delays technological and scientific advances by the avoidance of utilising disciplines that could help to face cyber security challenges [41]. Currently, cyber security should be addressed considering a set of different disciplines, technological solutions alone do not work any more, the need for additional measures has been recognised, for instance; organisational measures in a company can reduce the number of cyber incidents related with human errors and consequently improve cyber security in a organisation.

This work has identified three approaches for defining cyber security. The first, from the perspective of the information security properties known as classic bottom-up approach which seeks to protect confidentiality, integrity and availability of digital information, as in the case of Australia, Montenegro, Romania and Sweden in their NCSS. However, this approach could be considered weak because it cares for the protection of digital information, without considering additional measures and means essential to the cyber security field nowadays such as: political, economical, educational and organisational aspects and the protection against risks and threats in cyber space.

The second is the upon-down approach, which is based on the protection against threats and risk related with the use of cyberspace, it is the case of Germany, Finland and Belgium. Although this approach considers one of the principal states' concerns that is the protection in the cyberspace, it lacks due interdisciplinary considerations. The Colombian definition belongs to the later type however it adds a further element: to minimize the risks for citizens.

A third type could be said to be a mixed approach between an bottom-up and upon-down, when states attempt to protect themselves against threats in cyberspace and to consider information security properties and additional factors, as in the case of The Netherlands [14], including prevention and resilience but focusing on ICTs, Turkey [42] has also developed a keen interest in the protection of information systems. This category is considered as one of the best, however, according to this research it appears that the definitions developed by various countries lack certain elements, states develop their meanings according to their vision of cyber security, and subsequently their aims and needs.

Additionally, to respond to the growing cyberspace challenges governments have included new elements and disciplines to the understanding of the meaning of cyber security. Hungary incorporated, political, legal, economic, educational measures [43], The Czech Republic added organisational measures to protect public and private sectors as well as the general public [44], Austria followed a similar line, but focused on protecting key legal assets through constitutional means, although what defines a legal asset is not explicitly explained[45].

Finally, broader understandings have been published by governments such as The United States who are interested in establishing norms for regulating international behaviour in cyberspace, to protect intellectual propriety and online freedoms [46]; and also Japan, with the aim "*to ensure a free, fair and secure cyberspace"*[47]. Although there are clear differences among the national definitions of cyber security, there are also commons denominators; the following figure summarises and illustrates the findings:

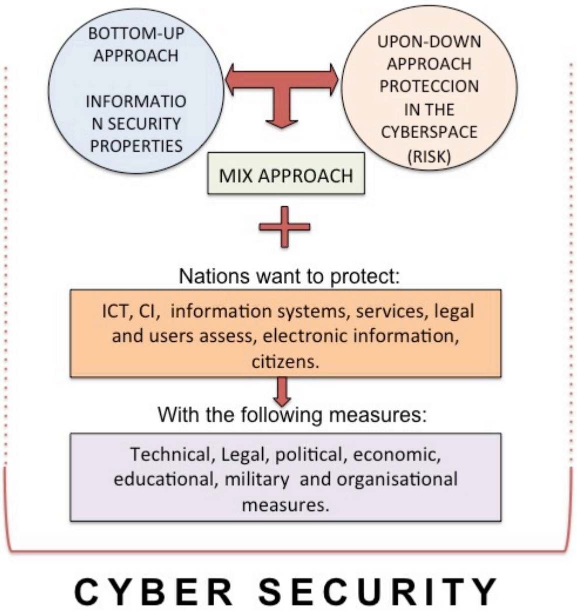
BOTTOM-UP APPROACH
INFORMATIO N SECURITY PROPERTIES
UPON-DOWN APPROACH PROTECCION IN THE CYBERSPACE (RISK)
MIX APPROACH
Nations want to protect:
ICT, CI, information systems, services, legal and users assess, electronic information, citizens.
With the following measures:
Technical, Legal, political, economic, educational, military and organisational measures.
CYBER SECURITY

Figure 2. Synthesis of Cyber Security Definitions.

3.1.1 Qualitative Analysis of an Online Questionnaire

An online questionnaire was distributed to 27 experts from 10 countries. The original instrument is in the Appendix I. The convenience group was selected because of the following criteria: to have at least a masters degree in cyber security or a related field, to have participated in the development of NCSSs, to have practical experience or to be a researcher in cyber security. These criteria respond to this research need of collecting information from experts who have knowledge in both fields the development of public policies and cyber security. The demographic data related to the questionnaire is shown in the Table 3:

Table 3. Demographic Data.

Country	Occupation	Age Group
Colombia	Big Data Analyst	Between 26-35 years
	PI Expert	
	Head of Information Technology in a Bank	
	Technology Analyst	
	Cyber security Manager Consultant	
	Cyber defence, Army´s officer	
	Cyber defence, Colombian Air Force Officer	
	System Engineer and a postgraduate student at the Andes University	
	System Engineer with a Master in Information Security	Between 36-45 years
	Head of Cyber defence Unit, Colombian Air Force	
	Dean of the master in cyber security and cyber	

	defence (ESDEGUE)	
	Chief Information Security Officer	
	Head of PONAL-CSIRT	
	Academic	More than 45 years
	Head of Public security and Infrastructure -NMD	
	CISO - Chief Information Security Officer	
Chile	Advisor MoD	Between 26-35 years
Estonia	Government official	
	Research Fellow	Between 36-45 years
Indonesia	Crypto agency in military strategic intelligent agency	
Hungry	Research - Employee	
Turkey	Senior Researcher	
The Netherlands	Director of Research	
EU	Specialist	
Finland	Director of Research	More than 45 years
	Director of Research	
Brazil	Chief of Joint Staff – Cyber defence Center	

The online questionnaire asked the experts' preferred definition of cyber security. According to their answers the major trend was a 29.62%, involving not only technological aspects but also non-technological such as: training, awareness, policies, procedures and good practices. These are the most complete answers due to show a broader understanding of what cyber security should be. Moreover, 14.8% of the experts define cyber security as a capacity of protecting systems to avoid any damage and the 11.11% as a condition, state or security level in cyberspace. However, the highest tendency with 33.3% of the answers was to avoid defining cyber security directly, this parameter matches with some countries' positions in which threats and risks in cyberspace are addressed without giving a definition at all, a summary of answers is shown in Fig. 3:

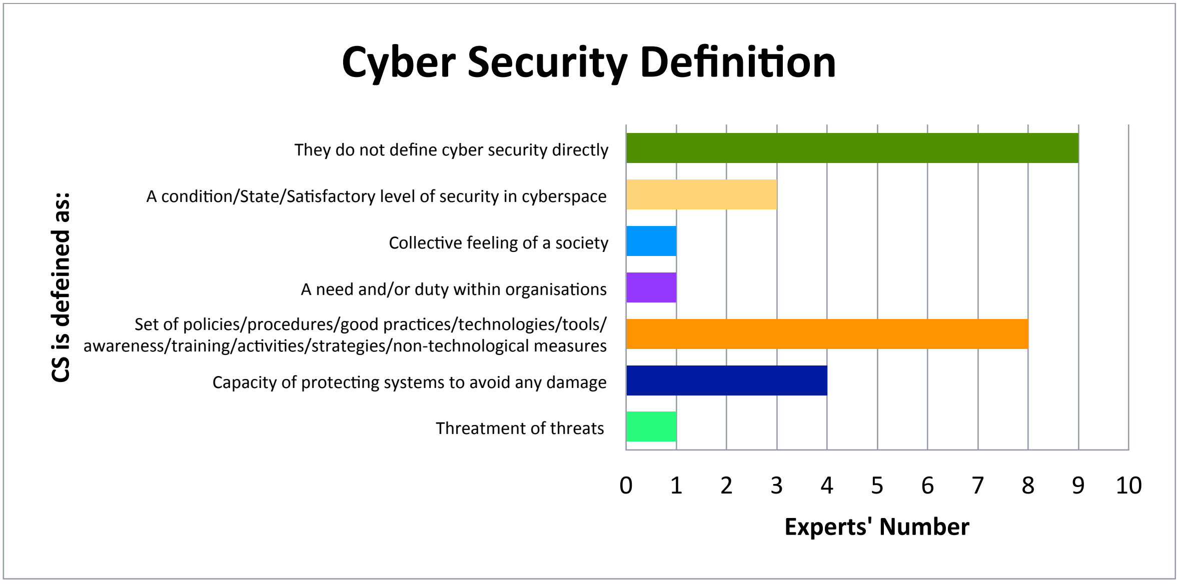

Figure 3. Summary of Experts Cyber Security Definitions.

The aim of cyber security also varied among experts' responses, although an strong similarities were present; 74.04% expressed that to protect the interest of states, CI, technological assets, users, security systems and/or data should be cyber security's objective. These answers show that cyber security is in charge of protecting more than digital assets but is necessary for keeping state's interest as well. The former tendency to define cyber security based on information security properties represent the 14.81% of the answers and the 7.4% do not express directly what they want to achieve through cyber security. Fig. 4.

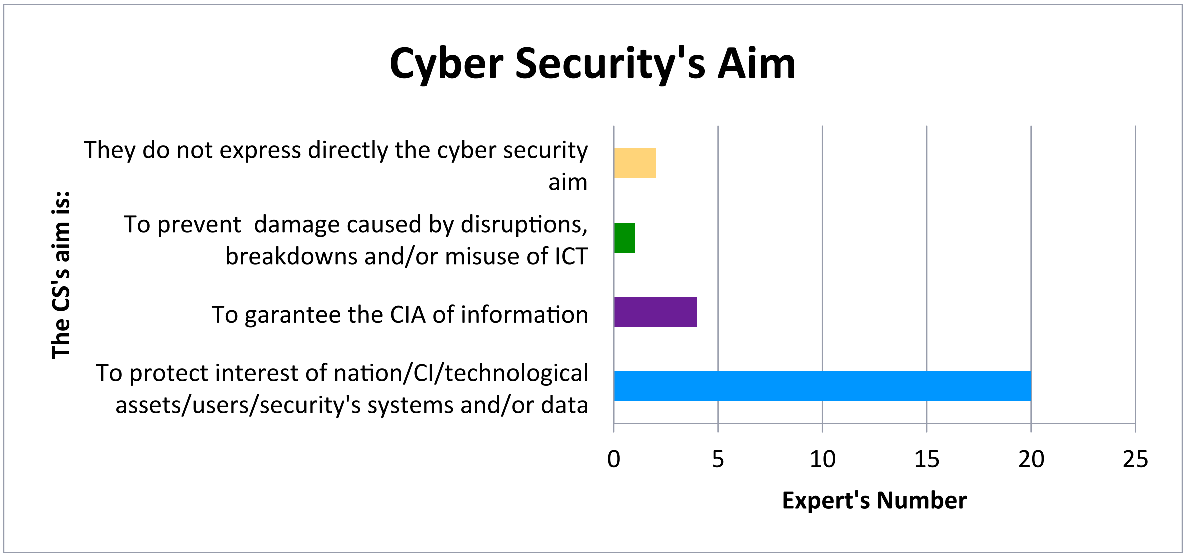

Figure 4. Cyber Security's Aims.

The experts' opinion matches with the comparison made among cyber security definitions. There is a lack of clarity of what cyber security constitutes and what it should involve. Cyber security is strongly related with the protection of diverse technological and non-technological assets and to secure national CI is the highest concern amongst the experts.

4 NCSS Comparative Analysis

This chapter compares the similarities and differences between the NCSS of Japan, the Czech Republic, France, Iceland and the Slovak Republic. Then it presents an analysis of findings. The comparison is focused on exploring how the selected countries face cyber security challenges and also identifying different aspects linked to cyber security policies. Subsequently determining the guidelines for the development of NCSSs, KPIs and minimum NCSSs components.

The strategies that were analysed belong to Japan, the Czech Republic, France, Iceland and the Slovak Republic. This selection was made according to the following considerations:

- The issuer countries must have a consolidated NCSS or similar public documents and these should be available online. Due to the online information represented the main source of information for this work. Additionally, there are states, which do not elaborate a NCSS itself but released other public documents according to their organisational structure or divide it into different documents, these cases were avoided into this research with the aim to achieve an homogeneous information's source;
- The issuer countries are members of the OECD. In order to align this research with the current Colombian political interest to the guidelines proposed by this organisation;
- The NCSSs selected for this research had to be published in 2015. In order to analyse the most up to date policies that have been developed. It brought into this work an outlook about how states address some of the latest cyber threats at national level;
- The selection had to be varied, consisting of strategies from countries that have diverse backgrounds, languages, economies, customs, population and so on. This allowed a broader observation and the identification of global tendencies in the development of NCSSs.

In the following sections there is a brief introduction to each country and a summary of the content of their NCSS. Then, a general comparison among the NCSSs including the similarities, key objectives, aims and vision that were presented by governments.

4.1 Iceland

Iceland is a Nordic nation with a population of less than 500.000, a parliamentary republic and one of the few states in the world that do not have standing armed forces since they gained sovereign control in 1918 [48]. Iceland is a NATO and UN member. The Icelandic National Cyber Security Strategy 2015 – 2026 addresses the government protection, economy, ordinary citizens and CI as a result of the growing cyber threats, with a vision of an "*Internet culture that is sound, promotes human rights, protects the individual and respects freedom of action to support economic prosperity and development"*[49]. It is focused on: an IT environment that has to be secure by design and private by design, computer-related education at all levels, strengthening security requirements on the market for software and related services, defence against cyber espionage, strengthening the legal framework, awareness rising, the infrastructure elements defence, the desire to have reliable systems and networks and to increase the collaboration with others countries and organisations. Furthermore, The Icelandic government set up for principal aims to reach their vision: capacity building, increased resilience, strengthened legislation and tackling cybercrime.

4.2 France

France is a semi-presidential republic, located in Western Europe with a population of more than 66 million in 2014. Currently, It is one of the most popular destinations for tourists in the world and is a European Union, and a UN Member. The French National Digital Security Strategy, released in 2015, is the second NCSS developed by French government. It establishes a set of policies against the following threats: Cyber attacks that target the state information system and CI, citizens and all kind of French business, cybercrime, cyber-malevolence acts and the loss of confidentiality, integrity or availability of essential information which can lead to "*economic losses, industrial accidents, and losses of human lives or ecological catastrophes and disturbances in public order, capable of affecting the life of the entire nation* [50].

The French NCSS has 5 principal aims: To ensure the defence of French fundamental interest in cyberspace, to protect digital lives of citizens and to combat cybercrime, to raise awareness training and education of digital security, to develop an environment favourable to research and innovation and make digital security a factor of competitiveness, and to lead with a voluntary European members states policies that promoting a safe, stable and open cyberspace.

The French government is aware of the need to distribute responsibilities among the stakeholders and established three groups: The first is responsible for recommending and implementing technologies, products and services; the second is responsible for protecting the state against digital pirates and also to implement cyber security policies; and the third is in charge of using responsibly the services and technologies.

4.3 The Czech Republic

The Czech Republic is a central European country with a population of almost 11 million in 2015. It has a unitary parliamentary constitutional government. Its economy is based on the agriculture, industry and services (CIA[7], 2015) and is NATO, EU and UN member. The Cyber Security Strategy of the Czech Republic 2015-2020 was released in 2015 with the aim to reduce cyber risks, mitigate threats and provide a secure, protected and resilient cyberspace. The Czech government considers organizational and technical measures to protect its systems and networks.

The Czech government calls for an efficient cooperation at national and international levels that involves public sector, private sector, academia and citizens. It highlights the transnationality of the field. The principal threats that their NCSS mentions are: cyber attacks, cybercrime, cyber terrorism and cyber espionage. In addition, eight main goals were defined: The efficiency and enhancement of all relevant structures (CI and IIS) and their protection; an active international cooperation as well as with private sector; research, education and awareness raising; to support the development of capabilities towards to combat the cybercrime and to develop a cyber security legislation.

4.4 Slovak Republic

Slovakia is a parliamentary representative democratic republic located in Central Europe with a population approximately of 5.4 million. It can be considered as a young country due to its separation from the Czech Republic in 1993. It is a NATO and EU member. In 2015 the Slovak Republic launched the Cyber Security concept for 2015 -2020. It is a national policy with the following strategic goal: "*to achieve an open, secure, and protected national cyberspace*" [51]. The Slovak government perceive cyber security as a

[7] For further information look at: https://www.cia.gov/library/publications/the-world-factbook/index.html, viewed on 01 May 2016.

key component of their national security and claims for the collaboration of public sector, private sector and academia as well as international organisations.

The cyber security concept of Slovakia is focused on protecting national cyberspace, security awareness, to involve all stakeholders in the implementation of the national cyber security policy, effective collaboration at national and international level and to guarantee the protection of privacy, basic human rights and freedoms. The concept proposed by the Slovak government in cyber security area contains seven measures to adopt and solve based on; international cooperation, communication and technical measures, to implement a cyber security education system and research.

4.5 Japan

Japan is an island located in East Asia with a population of 127.3 million; it has a parliamentary government with a constitutional monarchy. Japan is the third largest economy in the world, in terms of GDP after the United States and China, with high technology manufacturing, automotive and pharmaceuticals industries that are the economical pillars. The Japanese government issued the Basic Act on Cyber Security in 2014, that seeks to promote a cyber security policy; by establishing the basic principles of cyber security at national level, assigning responsibilities and roles among stakeholders, prescribing the cyber security concept, and determining the Cyber Strategic Headquarters as a command and control body of national security. In 2015 Japanese government launched its NCSS with the aim to ensure a free, fair and secure cyberspace, which addresses threats from the cyberspace use; from stealing personal, business and organizational information to threats against national safety and security through cyber attacks against CI.

This NCSS established five principles; the assurance of information flow with a secure cyberspace available for everyone, prevalence of the rule of law as in all other domains, and autonomous governance, based on multi-stakeholders' collaboration. Moreover, it describes in detail the four main goals and the direction of the Japanese policy: socio-economic improvement, a safe secure society, national security, and stability of the international community.

4.6 Comparison Among the Selected Countries

The NCSSs of the analysed states are mainly focused on; their socio-economic prosperity, defence and security, and the development of a security culture within multi-stakeholders. A summary of the facts taking into account by these countries and the similarities among them are presented in the Table 4.

Regarding cyber threats, these states have been found to have a long term vision and consider a big spectre of possible risks from the damage that a negligent service provider's employee can cause by mixing his/her personal life and professional life could contribute to losses in the confidentiality, integrity and availability of essential information and furthermore even economical losses [50], to the probability of becoming a victim of cyber terrorism [50][44][47]. Furthermore, the countries do not consider only technical threats. For instance, France introduces a new concept the "Cyber-malevolence", strongly linked to cybercrime and considered " *a digital aggression against people with results that are sometimes tragic"* [50].

Table 4. Comparison and Categorisation of NCSSs.

		Official NCSS				
Key Elements of the NCSS		**Iceland**	**French**	**Slovak**	**The Czech Republic**	**Japan**
Cyber Threats	Industrial espionage	X	X		X	
	Cyber Terrorism		X		X	X
	Cyber attacks	X	X	X	X	X
	Cyber-malevolence		X			
	The loss of CIA of the information		X	X	X	
	Cybercrime	X	X	X	X	X
Stakeholders	Government	X	X	X	X	X
	Academia	X	X	X	X	X
	Civil society	X	X	X	X	X
	Private sector	X	X	X	X	X
	International Community	X	X	X	X	X
Key action lines	Awareness	X	X	X	X	X
	Education	X	X	X	X	X
	Training		X	X	X	X
	Research and Innovation		X	X	X	X
	Legislation	X		X	X	X
	International Cooperation	X	X	X	X	X
	National Cooperation	X	X	X	X	X
	International Coordination		X	X	X	X
	National Coordination			X	X	X
	International Collaboration	X	X	X		X
	National Collaboration	X	X	X		X
	To increase resilience	X	X	X	X	X
	Minimum technical requirements	X	X	X	X	X
	Terminology (the need to develop a international term)	X		X		
	To protect CI, CII, IS or vital networks	X	X	X	X	X
	Personal Data protection	X	X		X	X
	To protect Digital live		X			
	Security by design	X	X	X	X	X
	To protect basic human rights	X		X	X	X
	Protection of privacy			X	X	X
	Protection of non CI, IS or vital networks	X	X		X	X

Additionally, countries do not specify which kind of attacks they should defend from, because the possibilities are innumerable and in constant change. However, they identified the following categories of cyber threats: cyber espionage, cyber terrorism and cybercrime. The loss of confidentiality, integrity and availability of the information is just considered by three countries, but Japan and Iceland indirectly count them among their responsibilities.

The global nature of cyberspace is more present than ever in the development of national policies; the need for collaboration, cooperation and coordination at all levels (national and international) is an imperative factor in the NCSSs analysed. Furthermore, all countries promote wide participation and involve different sectors: public and private, academia, citizens and the international community, although they are named and categorised in different ways depending on priorities, social distribution and policy implementation factors. For instance, France divides stakeholders into three different group as was explained in a previous section but call for a collaboration and cooperation in as much as possible.

Cyber Security is considered an issue of national security, a vital component of national socio-economic development and essential for preserving national and international stability. Additionally, states know about the importance of CIs, CII, IS or vital networks but currently are also aware of risks and threats related with small and medium companies because are frequent targets of cyber attacks or victims of cybercrime.

Supporting the same need for global measures, states call for diverse ways to work with multi-stakeholders not just in a cooperative way, they also are seek for collaboration with the exception of the NCSS of the Czech Republic. Coordination at national and international levels is also present in the NCSS of Slovakia, Czech Republic and Japan. An effective teamwork would support the countries in a vast range of areas, such as: political, organizational, legal, technical, and educational. It is considered essential to combat cybercrime and to keep international stability. France goes a step further in this field through the fifth objective: "*Along with voluntary Member States, France will be the driving force behind European strategic autonomy. It will play an active role in the promotion of a safe, stable and open cyberspace*"[50].

Academia and civil society are broadly named in the NCSSs revised. Academia as a source of knowledge and committed to a sustainable development; would lead countries towards ethical innovation and research in cyber security fields. Citizens are the final users who are members of a digital society as well. Closely related, awareness, training and education are some of the biggest challenges than countries mentions in their NCCSs with the exception of Iceland that does not tackle this aspect directly. States propose to incentivise awareness, to train specialized people with the required cyber security skills to be able to prevent, mitigate and react to cyber attacks. Furthermore, to established policies for educating people at different levels even developing an educational system active from primary school to postgraduate studies level. In addition, governments request companies to practice the concept of "Security by design", which invites companies to consider cyber security issues from an early stage in the development of products and draw an emphasis on; new national services and products that should be safe from their conception and production. Another common point is the concern over data protection, excluding Slovakia that talks about privacy protection instead. A broader vision is presented by Japan, Slovakia, Czech Republic and Iceland on the protection of human rights if to compare theirs with the French strategy that is the only one of the five that seeks for protecting people's digital lives.

The protection of CI, CII, IS, or vital networks is one of the main purposes of the NCSSs analysed. However, states recognise that they need more than technical measures to ensure protection for example; organizational, legal, and educational aspects should be also taken into account. Furthermore, states acknowledge that it is not enough to protect vital services and infrastructures; it is also essential to safeguard non-critical infrastructure and non-critical information systems. Japan even demands the protection of the society in which the Internet of Things (IoT) system prevalence.

4.7 Guidelines, KPI and minimum NCSS's Components

This chapter explains the guidelines and KPIs for the development of NCSSs as well as minimum components that a national strategy should contain in the cyber security field. This outcome is based on the interdisciplinary literature review, document analysis, and the conclusions drawn from the analysis of the online questionnaire. The comparison developed in the previous chapter is also considered a trend to follow to the extent of the common denominators that were found and the innovative aspects that some of the NCSSs advanced.

States expect to involve all stakeholders including international sectors into the development and implementation of NCSSs. Moreover, collaboration, cooperation and coordination are considered essential in cyber security field. Hence, this research proposes a hybrid approach for the NCSS development as a method to implicate the widest number of stakeholders possible. The proposal that that this work supports, brings up the positive factors related to the Bottom-Up and Top-Down approaches and mixes them with Deming's management model. However, the last phase of the Deming's model was changed in order to match with the proposal guidelines, because it is applied exclusively to the NCSS development and focused on reaching cyber threats addressed by the selected countries (Japan, Iceland, Czech Republic, France and Slovak).

Governments normally lead the development of cyber security strategies at national level, but which organization is by itself a differentiator because states have different structural arrangements. For instance, in France the Prime Minister lead the cyber security policy with the support of the Information System Security Strategy Committee and under the supervision of the Secretary General for the Defence a National Security (CCDCOE, 2015)[8] whereas in the Czech Republic the National Security Authority - NSA has the overall responsibility for national cyber security supported by other subordinated organisations. (CCDCOE, 2015)[9] The Icelandic National Cyber Security was developed under the leadership of the Minister of the Interior.

As illustrated earlier, states have different organisations and work according to them. However, the most important factors are that the office in charge of the NCSS's development has governmental support, enough knowledge in the Cyber Security field and related areas or has access to it, and the authority to congregate all stakeholders. This research applies all encompassing terms that can be adapted to any particular governmental structure in the development of NCSS, due to the guidelines for the development of NCSS were developed under the principles of transferability and adaptability.

[8] For additional information look at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_FRANCE_032015.pdf, viewed on 01 May 2016.

[9] For additional information look at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CZE_032016.pdf, viewed on 01 May 2016.

4.7.1 Qualitative Analysis of an Online Questionnaire

The online questionnaire asked the experts' for stakeholders that should participate in the formulation of NCSSs. 88.8% of participants recognised that the public sector must participate in the development of NCSS and lead it process. The need to call private sector and academia is broadly accepted as well with 77.7% and 74% respectively. Finally, experts agree in a 55.5% that civil society should participate in the development of NCSS. Although the group of experts seem to be aware of the transnational nature of the cyber space, just 11.1% of them express that international organisations, international experts or other countries should be part of the NCSS's development. Fig. 5.

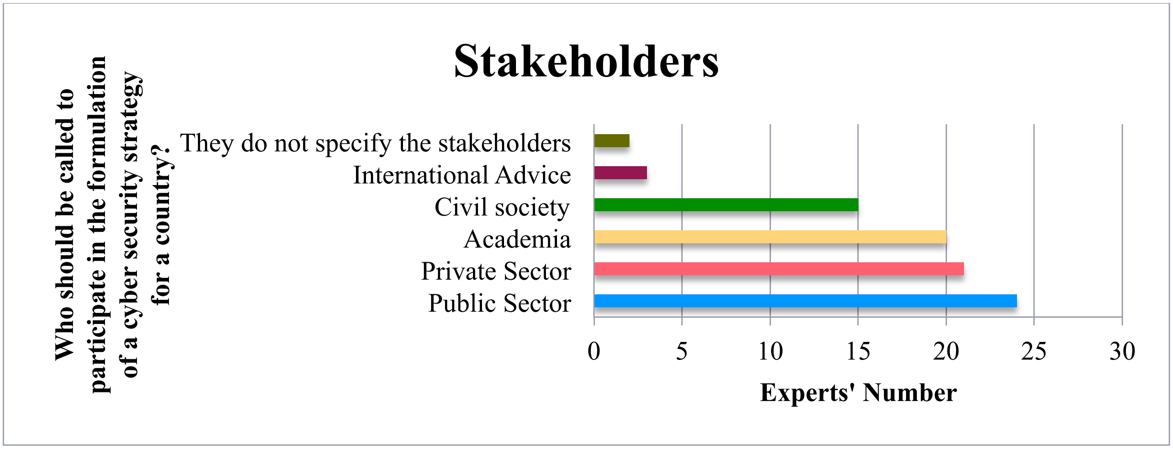

Figure 5. Stakeholders Who Should Participate in the Development of NCSSs.

A multi-stakeholder collaboration for developing a solid NCSS was reiteratively advised by the group of experts; at least representatives from public and private sector, academia and civil society should receive the call to participate in this development. Moreover, they strongly underline that each country has a particular situation and it should be analysed for being able to choose stakeholders who would participate, as generalisations do not work. Although to follow countries with successful experiences brings useful information, policymakers have to be aware of the particularities of their country for measuring the correct level of participation and ownership.

If there is any standard used to develop NCSSs, was asked to the group of experts; 51.8% of them agree that countries do not follow any special methodology, states normally go through an empirical process supporting mainly by national and international experts or agencies and allies countries with a successful experiences in cyber security area. Additionally, states should focus on the particular situation of their country due to the NCSS should be aligned with their legal, political, economic, military and social reality.

Although 33.3% of the experts recognise that there are international standards for the development of NCSS (NATO, OEDC, ITU) and 14.81% responded with standards with do not specifically focused on NCSSs' development, they agree that cyber strategies do not go into details regarding to any standards and in some cases it is the result of a political exercise, which constitutes a trouble due to the final NCSS sometimes differs of what the country really needs in addition the 51.85 % directly expressed that states do not follow any standards as is showed in the Fig. 6. At this point the need arises to help states in the development of their NCSS; through a set of guidelines; KPIs and minimum components; all of them with adaptable and transferable characteristics.

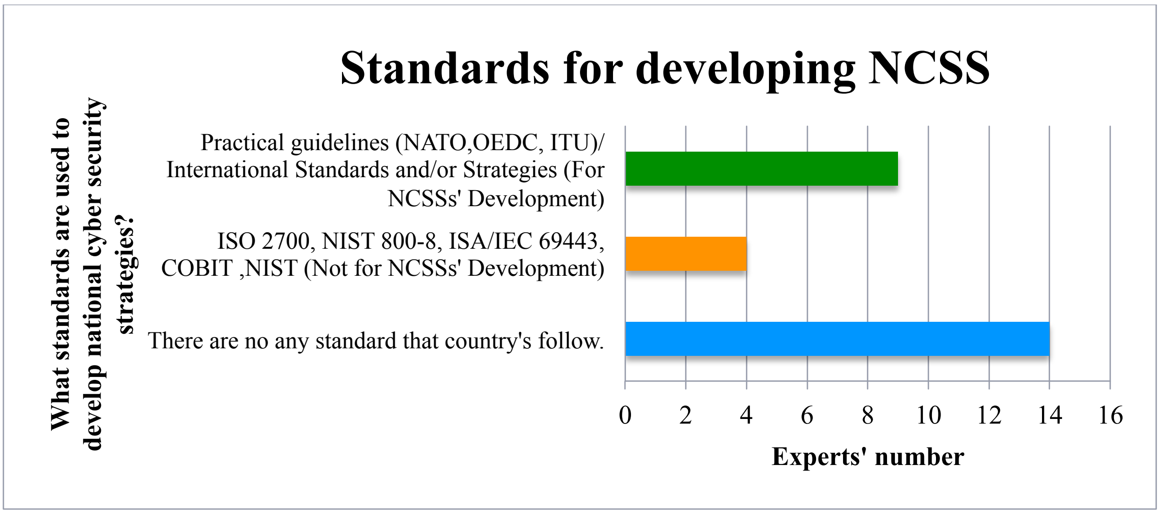

Figure 6. Existing Standards for the Development of NCSSs.

Furthermore, this work found a set of problems and obstacles that countries face in the formulation of a cyber security strategy, 70.3 % of the experts' group considers that contradictory interests among stakeholders and the lack of clear responsibilities and roles and their definition exists amongst them, this represents the most difficult issue to resolve during the development of NCSS. Followed by 51.8% of participants who think that economic limitations affect meaningfully this process. An additional concern is the lack of preparation and methodology or expertise present in the formulation process, sometimes it seems an untidy process and without a final objective. This obstacle could be solved through strong leadership by the agency or person in charge of developing a NCSS, which must be basis for guidelines as the proposal through this work and a continuous supervision of the process through an a KPI and additional measures. Fig. 7.

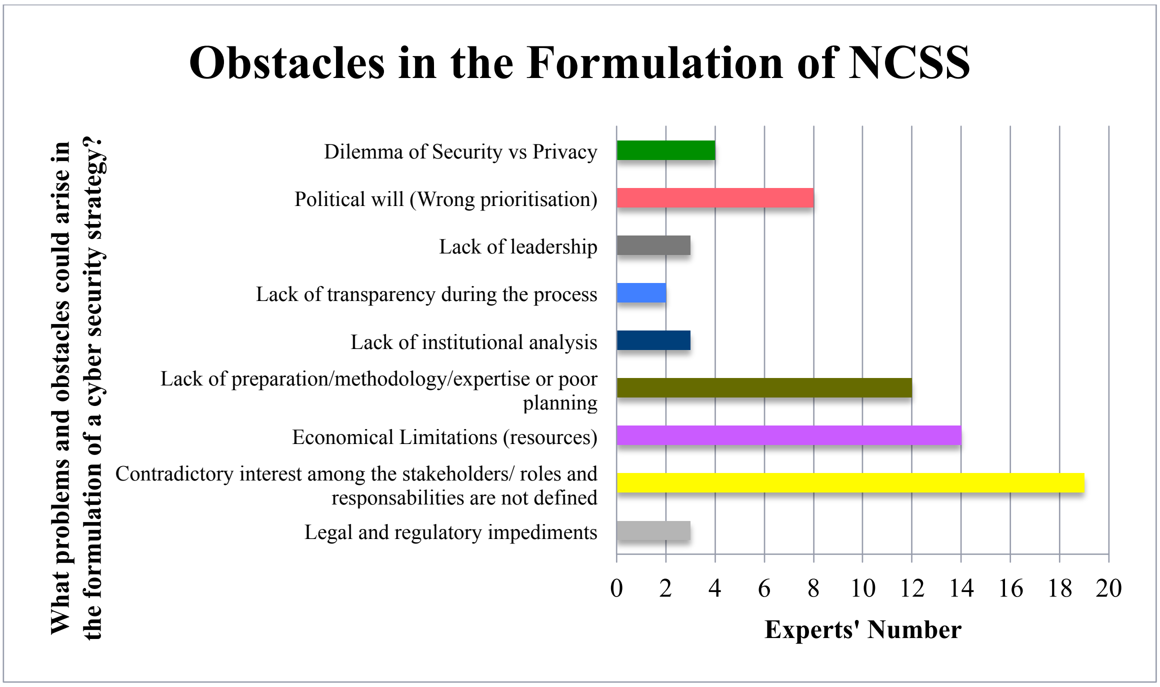

Figure 7. Obstacles in the Formulation of NCSSs.

Political will that may lead towards erroneous prioritisation is also a concern amongst the experts group, although it is difficult to analyse from the academic point of view, it is highly recommendable to take into account a national risk assessment framework that states what the actual risks and threats in cyberspace are, while helping to resolve dilemmas such as the one posed by the difficulties balancing security vs. privacy.

4.7.2 Guidelines for the Development of NCSS

The set of guidelines applicable to the development of NCSSs proposed in this work could be adapted to the particular situation of each country, and could be taught to suit to any state. It is composed by four phases; Plan, Do, Check and Legalise. Additionally, each phase is subdivided into several steps as is shown in fig. 8:

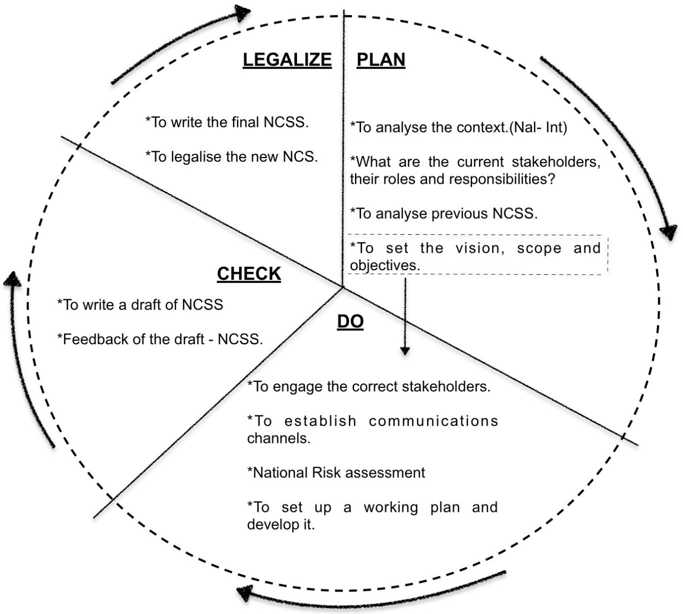
LEGALIZE
PLAN
*To write the final NCSS.
*To legalise the new NCS.
*To analyse the context.(Nal- Int)
*What are the current stakeholders, their roles and responsibilities?
*To analyse previous NCSS.
*To set the vision, scope and objectives.
CHECK
*To write a draft of NCSS
*Feedback of the draft - NCSS.
DO
*To engage the correct stakeholders.
*To establish communications channels.
*National Risk assessment
*To set up a working plan and develop it.

Figure 8. Guidelines for the Development of NCSSs.

The following elements were found to be common in the NCSSs of the selected countries (Japan, France, The Czech Republic, Iceland and Slovak) and the online questionnaire:

- To enhance a multi-stakeholder cooperation, collaboration and coordination at national and international level;
- To promote awareness, education and training in cyber security field. Moreover, to support the research and innovation;
- To strengthen the legal framework;
- To increase resilience against cyber attacks;
- To protect CI, CII, IS or vital networks;
- To include data protection (personal or organizational) and privacy considerations.

This research proposes a mixed approach in order to involve a wider range of stakeholders and to diversify the gathered information techniques; it consists in tackling cyber security issues at national level considering diverse stakeholders and perspectives. The organ in charge of the NCSS's development would lead the process as a coordinator; the aim is to know both perspectives and to avoid overlapping efforts. On one hand, there is a centralised national agency responsible for cyber security but the leader of the NCSS's development with the national organisations related to cyber security. On the other hand, multi-stakeholders starting in low levels and going up. It would help to resolve one of the problems identified in the formulation of NCSS the lack of an accurate participation. Fig. 9.

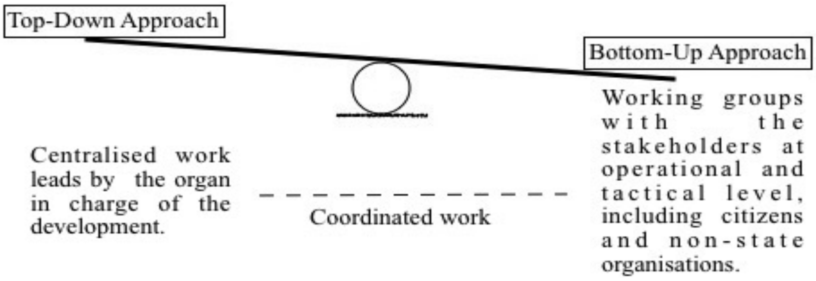
Top-Down Approach
Bottom-Up Approach
Working groups with the stakeholders at operational and tactical level, including citizens and non-state organisations.
Centralised work leads by the organ in charge of the development.
Coordinated work

Figure 9. Mix Approach for the Development of NCSSs.

The situation of each country is unique, so generalisations do not apply. Structures, states responsibilities distribution, national interests and performance of each state vary and could be studied to shape policies of real impact through conceptual evaluations, document analysis and interpretative analysis. According to the information gathered through this research, it presents a minimum set of stakeholders, the given names are considered generic and the selection was made based on the possible functions that these are responsible for. Table No. 5

Table 5. Possible Stakeholders.

Sector	Possible Stakeholders
Public Sector	▪ National Planning Department ▪ Ministry of Interior ▪ Ministry of Justice ▪ Ministry of Foreign Affairs ▪ Ministry of National Defence ▪ Ministry of Education ▪ Ministry of Information Technology and Communications ▪ Ministry of National Treasury ▪ National CERT ▪ Military Forces ▪ Intelligence Services
Private Sector	▪ CI's managers ▪ Small and Medium Enterprises ▪ National unions and associations related to cyber security ▪ Sectorial CERT – CSIRT
Academia	▪ Universities ▪ Think-tanks ▪ Research centers
Civil Society	Organisations or institutions that represent citizens could be an option for guaranteeing their involving into the development of NCSS.

Depending on the country, the Representatives from *International Community* may be considered in the development of NCSS. A government could request international advice from organisations such as OAS or the UN. It would translate in the strengthening of cross-boarding vision of cyber security.

An additional explanation with a summary of the proposal guidelines is in the table 6:

Table 6. Guidelines for the Development of NCSSs.

Phase		Description
1.1	To analyse the context at national and international level.	▪Political will and National interest. ▪Economic country situation. ▪National security goals. ▪International threats and concerns. ▪ Society and culture of the country. To be aware of the context in which the NCSS will be developed and implemented. It seeks that the stakeholders particularise the development and adapt it into the national situation and interests.
1.2	To investigate the current stakeholders roles and responsibilities.	Who is in charge of want sometime differs to how it responsibilities are written down. Leaders of the development process have to be clear about the roles and obligations of each stakeholder prior to implementation; it applies a global vision about the current national situation in the cyber security field and related areas. Besides it is essential for choosing the stakeholders who will participate in the NCSS's development.
1.3	To analyse the previous NCSS.	When previous NCSS or similar documents exist, it is vital to analyse their particular characteristics and the real impact of these for the country. ▪Was the action plan accomplished totally or partially? ▪What were the weaknesses and strengths of the previous NCSS? ▪What lessons could be learned from the previous development process and implementation?
1.4	To set the vision, scope and objectives	It allows to keep the focus and to work collaboratively in order to achieve the same final aims. It is recommendable to set them up in common agreement with stakeholders. However, the relevant parts normally have quite diverse interest whereas the interest of the private sector ISP's is very different from those of the intelligence interests and could become contradictory even inside of the public sector the military forces' position normally is quite far from the priorities expressed by the ministers of technologic and economics. In addition, not all stakeholders have the same sense of urgency and therefore to prioritise the objectives represents a discussion that could end up in an unsatisfactory manner for some stakeholders.

2.1	To engage the correct stakeholders	The digital domain comprises an abundance of parties and actors who have become increasingly connected to each other and dependent on each other. In order to be able to act safely in digital domain, which is characterised by a great dependence between the parties, it is important for citizens, organisations and government bodies to actively participate based on a clear allocation of roles and a great degree of transparency. Although, governments who identified their Critical Infrastructures can use this information to select the participants in the development, it process should be wider and include diverse social, economical and political sectors.
2.2	To establish communication channels among the stakeholders	Due to the number of stakeholders which should participate in the development of NCSS it is important to set up the manner, mechanism and means that stakeholders would use to communicate to each other, to express their views, points of view and needs. The information shared should be exclusively for the formulation process, and leaders of it (public sector) should guarantee the security of shared information and means using for this process. Additionally, non-disclosure agreements might be signed if needed.
2.3	National Risk Assessment	It technically allows identifying, analysing and evaluating the actual risks [34]. Moreover, it brings useful information for the objectives' selection and prioritisation as well as to set the scope that would cover the strategy.
2.4	To set up a working plan - with the stakeholders and develop it.	It is important to set up rules under which stakeholders would work. To guarantee participation of all stakeholders and reach agreements in the points that they could disagree. A leadership of the organisation or office in charge of the NCSS's development is also important for solving issues, to keep the track towards the aims and vision established in the previous steps and to ensure that the process is in continuous evolution.
3.1	To write a draft of NCSS	When the stakeholders reach minimum agreements, policy makers in a parallel process should convert them into a document that have to reflect clearly the work done. The document will be in constant change until a final approval is signed.
3.2	To do a feedback of the work based on the NCSS draft.	It is essential that the real work does not differ from the written policy, before the final approved the document the NCSS should be re-write a number of times until the majority of stakeholders are in agreement. Nevertheless, its process could be endless and the organisation or office in charge of leading the NCSS development have to take the final decision about which point its process should finish if

		all the stakeholders do not fully agree.
4.1	To write a final NCSS	All the work has a final aim; to write a NCSS for a specific country, It has to be clear and according to the result gotten from the previous steps.
4.2	To process the NCSS according to the law.	Each state has a particular process to legalise their national strategies, after the developmental process ends, the final text should go through this process and become an official NCSS.

4.7.3 Key Performance Indicators

This work determines KPIs for the development of NCSSs, which are focused on determining success and quality in achieving the final strategic goal [31], which is to develop a NCSS with the particularities of each state. Additionally, the information gotten from the NCSS comparison and the proposal guidelines were taken into consideration to align them into a single process. These were taught as qualitative measures, and then these are not questions of past and fail but a better understanding of the formulation process to aid the success of new NCSS. In order to provide guidance to policymakers this work proposes tables to help them to identify if the KPIs are being accomplished or which are their actual state of development. It is important to underline that the proposal tables might be modified according to each state requirements then policymakers could add and/or subtract variables to fulfil their needs.

1. To consider the context under which the NCSS will be developed. Refers to the economical, political, social, legal and military situation of each country. Furthermore, policymakers should consider previous policies, others national strategies and international agreements. Table 7.

Table 7. KPI No 1.

	Variable	Yes	No	Partially	Why?	%
To analyze and consider how these factors affect the formulation of a NCSS	Political requirements					
	Economic resources available for policy development and implementation					
	National security goals and threats					
	International situation (Threats, concerns and agreements)					
	Society (Culture and Customs)					
	Legal demands and/or requirements					
Total:						

This work suggests 6 variables to measure the KPI No 1; each task has a maximum value of 16.67% as a result of dividing 100% among number of variables (6). However, policymakers might increase or decrease number of variables, in that case maximum value of each task would change. If a state does not totally fulfil a task, a minor value has to be assigned (<16.67%). The calculated values of each task should be added to get the final KPI's value; it should be assigned between 0 % and 100%.

2. To establish the vision, objectives and scope in mutual agreement with the stakeholders and to set priorities and limitations considering the result of a national risk assessment and national interests. It brings objective factors into the development process and to focus on the actual reality of the country. Moreover, it purports that stakeholders work collaboratively to the same ends and to avoid working on topics that will not be considered in the NCSS of each country. Table 8.

Table 8. KPI No 2.

	Variable	**Yes**	**Not**	**Why?**	**%**
To establish (For a specific time)	Vision				
	Scope				
	Priorities				
	Aims				
	Limitations				
	Have been the vision, scope, priorities, aims and limitations shared with stakeholders?				
Total:					

To calculate the KPI No 2 this research proposes 6 variables with a 16.67% of value for each one if the answer is yes, otherwise it would get 0%. These percentages may change if policymakers decide to add or subtract any variable, in this case were calculated in the following way: 100% divided into 6 (number of variables). The partial values have to be added to get the final measure.

3. To involve the correct stakeholders into the development process from the beginning is one of the challenges that policymakers commonly face. Based on the comparison realized in the previous chapter countries are interested to direct their NCSS, towards a broad spectrum of stakeholders from public, private and international sectors as well as academia. Then, if the states want a major acceptance of their policies and to accomplish them effectively, states should achieve a higher degree of stakeholders' participation and strategy "ownership" during the development process [20]. Table 9.

   This work suggests 22 stakeholders that should participate in the formulation of a NCSS. Nevertheless, the participants' number could be changed by policymakers to fulfil state's requirements; each representative gets 4.54% as a result of dividing 100% among number of stakeholders (22), if there is any office/organisation that does not have any representative it would get 0% but if there are more than one from the same office/organisation a 4.54% would be assigned. These values should be added to get the final result to the KPI No 3. Finally, to keep level of participation over to 75% is highly recommendable in order to guarantee that the stakeholders' majority is involved in the NCSS's formulation process.

Table 9. KPI No 3.

	Representatives from	**Yes**	**No**	**Why?**	**%**
Public Sector	National Planning Department				
	Ministry of Interior				
	Ministry of Justice				
	Ministry of Foreign Affairs				
	Ministry of National Defence				
	Ministry of Education				
	Ministry of Information Technology and Communications				
	Ministry of National Treasury				
	National CERT				
	Military Forces				
	Intelligence Services				
Private Sector	CI's managers				
	Small and Medium Enterprises				
	National unions and associations related to cyber security				
	Sectorial CERT and/or CSIRT				
Academia	Universities				
	Think-tanks				
	Research centers				
Civil Society	Organisations of community leaders				
	Citizens				
International Community	Organisations and/or Institutions				
	States				
Total:					

4. To set up a working plan and develop it. According to the proposed guidelines this KPI measure the phases 2.2 and 2.4, which are about establishing communication channels and to develop a working plan with stakeholders. It seeks that the development process has a constant level of participation and evolves in perpetuity. Then stakeholders have to agree on a roadmap; normally they might establish a set of meetings for discussing grey areas and to expose their points of view. It is highly recommendable to keep track of the aims and visions set up previously and to use technology for efficient gathering information. Table 10.

   In order to calculate the KPI No 4, this research proposes 6 variables that can be adapted according to a specific NCSS's formulation process. Each variable should be evaluated between 0 % and 16.67% but if the number of variables changes this range would change as well. Policymakers have to objectively evaluate the proposal variables in line with the work done. Finally, the total is calculated by adding all partial values.

Table 10. KPI No 4.

	Yes	Not	Partially	Why?	%
To schedule meetings and/or workshops					
To assign specific tasks to be developed during meetings and/or workshops					
To do partial reports about developed activities					
To set communication channels					
To establish partial aims for being reached at specific time					
To keep stakeholders participation level as high as be possible through the process (at least 75% is recommendable)					
Total:					

5. To balance the different interests of the stakeholders. As a developmental process, which involves stakeholders from different backgrounds and interests to reach commons points is hard work. There are some dilemmas that have been identified by NATO in 2012 such as: Economy vs. National Security, modernisation or CI protection, data protection vs. information sharing, and Freedom of Expression vs. Political Stability [8]. These are a few examples of the discussions that would be part of this process, *although a final decision is considered a political one.* However, it is recommendable from the academic point of view that the vision, objectives, scope and limitations established during the previous phases would be considered for taking final decisions. Finally, prioritisation plays a vital role at this point, although the needs among countries could be similar, looking in a deeper way the priorities and resources are different.

4.7.4 Minimum Components of NCSSs

This research also proposes the minimum components of a NCSS, and by minimum it is meant; a set of elements that should be part of a NCSS, these would allow that stakeholders at national and international level to know what exactly a government wants to achieve through their cyber strategy. It also would help to enhance the international cooperation and to avoid misunderstandings. Table 11.

Table 11. Minimum Components of NCSSs.

Component	Description
Foreword	For establishing the importance and value of the NCSS.
Introduction	Introducing the NCSS, outlining the relevance and the most important aspects related within the strategy.
Vision	To explain what a state ideally wants to achieve long-term in cyber security area.
Principles	Explaining the foundation on which a strategy would be developed and the criteria for orienting the NCSS.
Main Goals (aims)	Explicitly, define what a state would accomplish, where all stakeholders efforts (and needs) would be set out too.

Action Plan	It is the roadmap that would bring into reality the NCSS. These should be concrete and clear. It is highly recommended that assigned tasks have a single point of responsibility for development and a specific time for accomplishing them. These would be useful for measuring the NCSS's implementation

Depending on each nation the NCSS could add sections as the Japan's case or take away others ones as in the case of France. Besides, it is important to underline that this proposal is about the minimal content of NCSSs, it is not referring to the organisation or sections of the strategy itself, due to this it is quite natural that national strategies may differ as a result of the diverse particular characteristics of each country [3].

5 Colombian Case Study

This chapter applies the guidelines proposed to the particular case of the Republic of Colombia, starting from the description of cyber security status in Colombia, followed by recommendations and limitations. This section relies mainly on offline documents and public information.

5.1 Cyber Security in Colombia

The case study begins with the steps that correspond to the first phase of the Guidelines for Developing NCSS, named as PLAN, these are: to analyse the Colombian's context under which the NCSS would be implemented *(Phase 1.1);* to investigate what are the current stakeholders' roles and responsibilities *(Phase 1.2)*; to analyse the earlier versions of the Colombian's NCSS *(Phase 1.3)*. Finally, to set a vision, scope and objectives *(Phase 1.4)*.

5.1.1 Factors that Affect the Development of a Colombian NCSS – Phase 1.1

The Republic of Colombia is a Northern South American country with a population of more than 48 million, with a governmental system, which is based on a presidential participatory democratic republican framework. It is dependent on multiple agro-manufacturing sectors with various industries such as: oil, agriculture, fisheries, industry, mining, services and energy. On the other hand, according to the Report on Cyber security and Critical Infrastructure in the Americas by the OAS: "*The income of the Colombian ITC's industry reached €14 billion euros in 2012, 6% of the GDP with an annual growth of 9%. The ITC industry created 110,000 direct jobs and it's growing faster than others. The investment in the ITC sector reached €5.9 billion euros in 2013"*[52]. It means the IT impact over the Colombian economy can be considered high.

However, the governmental priorities seem to be far from the development of an adequate cyber security plan. It is explained that Colombia has been highly affected by the drop in oil prices, and since it represents a big percentage of the state incomes the budget does not allow investment in the ICT's sector. Additionally, on September 2012, the Colombian government officially established a negotiation with one of the oldest guerrillas around the world known as FARC-EP, and it constitutes a state priority. The government assigns a big part of the national budget to support this process that should conclude according to official declarations in the present year and for futures requirements that would be the result of the final peace's agreement. It is estimated that the cost of billons of dollars has derived in loss of opportunities and also reduced the capacity to advance in other areas of vital interest. The Colombian President established budget limitations to all governmental bodies in the begging of 2016 and a study for incrementing taxes is on the way. From the economical perspective the next Colombian's NCSS should be issued under an austerity perspective. Then the aim's prioritisation would play an important role.

The outlook for Colombia is undergoing a transformation process. Some predictions should be considered: for the development of the NCSS: the state interest is to be member of the OECD, expressed from 2013, this organisation requires that Colombia satisfies a minimum of global standards in different areas including cyber security. Then, is highly likely that policymakers would follow the practical guidelines released by this organisation in 2015. It also important to underline that there are not global solutions for improving cyber security at national level. The OEDC talks about enhancing the social and economical benefits related with cyberspace. But even though this vision may be aligned with Colombian policies, in practical terms its applicability presupposes a level of social and economic development that cannot be said to match the local circumstances. It is highly recommended that although the country follows a particular guideline, it should to be made to suit/adapt to the actual Colombian situation.

5.1.2 CONPES-3701 and Stakeholders' Roles – Phase 1.2 and Phase 1.3

Some measures have been established to improve the level of cyber security in Colombia. Starting with the previous cyber security strategy known as CONPES-3701 is a document that was released in 2011 under the leadership of the National Planning Department, and contains the national guidelines for cyber security and cyber defence. Its chief objective is to "*fortify the capability of the state to meet the threats that attack its security and defence in cyberspace*" [18]. The national strategy took into consideration several factors discussed earlier and common to other countries: human resources, international cooperation and legal reforms but placed the initial emphasis on the development of the police and military capabilities [53].

Following the policies determined by the CONPES-3701, some governmental organizations were established: an Inter-sectorial Commission in charge of formulating a national strategic vision in the cyber security and cyber defence areas; the Colombian Cyber Emergency Response Team (ColCERT) with the responsibilities of a national CERT; the Armed Forces Joint Cyber Command (CCOC) and the Police Cyber Center (CCP) mainly in charge of combating the cybercrime in Colombia. In addition, the Colombian government assigned $16.428.444.328 Colombian pesos for the policy implementation. Fig. 10.

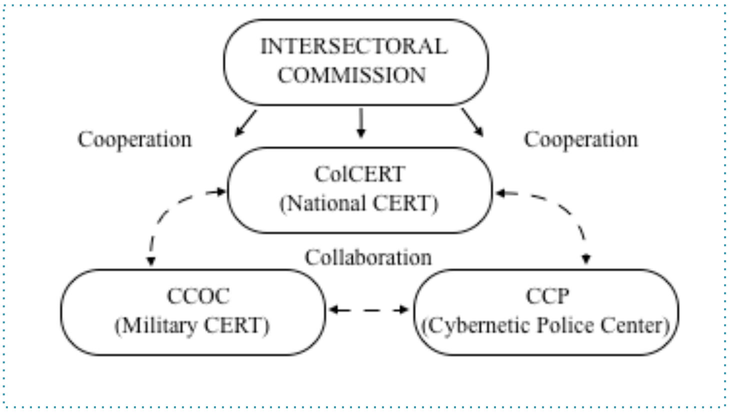

Figure 10. Coordination Model Established by the CONPES-3701.

These emerging institutions created by the CONPES-3701 are in place as new public sector stakeholders but there is lack of clarity as to who is responsible for what. The intersectoral commission does not have an active role; there is no register about the meetings, activities, recommendations or guidelines that they have developed during the last couple of years. The military CERT and the National CERT do not have enough resources for building capacities; there are fewer trained people than what is needed, the technological infrastructure is inadequate and resources are insufficient. From the private sector this analysis is more difficult to conduct. Although the Colombian NCSS ordered the CI's identification, this process does not advanced. Currently there is only a generic list of which could be the Colombian CIs. Then, to extend the private participation to SMEs or non-CI is currently complicated for policymakers, but there are some factors, which would help to engage additional stakeholders such as: economic or social impact. From the academia, one of the most prestigious Colombian universities (Andes

University[10]) has constantly participated in cyber security activities at national level. However, it is necessary that the academic participation increases towards more universities due to Colombia has more 200 universities, it means that the level of academic participation in the formulation of the NCSS is low. To involve experts from different disciplines, research groups and think thanks, is also necessary.

Colombian' government is aware of the importance of International Cooperation as an instrument for enhancing cyber security at national level. Following the Report of the Secretary-General of the United Nations (30-JUN-2014), Colombia agreed with being part of the OAS General Assembly resolution AG/RES 2004 and the declaration known as: Strengthening Cyber-Security in the Americas in 2012. Moreover, the OAS created the Inter-American Committee against Terrorism (CICTE), which is responsible for supporting the development of cyber security capabilities inside the member states. Colombia in addition, joined the multilateral agreement with the World Economic Forum: "Partnership for Cyber-Resilience". All these international commitments generate state responsibilities that have not been detailed. So far, these remain statements of good will on paper.

Additionally, Colombia also has reached agreements with international companies and organizations that operate in the information and communication industry such as: Microsoft, which allows access to the Cybercrime Center; and the Anti-phishing Working Group, which gathers a global coalition of legal authorities, industry enterprises and Government entities for establishing efficient cyber incident alerts and response mechanisms. In 2013, Colombia formally applied for being member of the Budapest Convention on Cybercrime.

Colombia's citizens are often victims of cyber criminals. According to the OAS almost half of the phishing attacks in Latin America occur in Colombia and the most frequents cybercrimes are: phishing, electronic fraud, use of malicious code, computer hijacking, hacktivism, identity theft and cyber espionage [52]. The National Police reported an increase of almost 50% in the number of people arrested for cybercrimes or illegal activities related to cyberspace from 2011 till 2013 the increase still boosting during the last years. Even, some well-known cases as President Juan Manuel Santos' personal e-mail suffered an attack that consisted of hacking and identity theft.

Regarding cybercrime the CCP has developed several strategies for decreasing the impact and amount of cybercrimes in Colombia. Nowadays it operates with tools, such as; Virtual Contact Point for reporting cybercrimes online, which is available 24/7; specialized laboratories (forensic informatics) and PROTECTIO software for parental control. An awareness campaign is in implementation; it is based on releasing cyber security guidelines and reports for cybercrime prevention. Furthermore, the CCP is the national contact point with EUROPOL and INTERPOL. According to the Colombian Superintendency of Industry and Trade, the legal framework to regulate activities in cyberspace and to combat cybercrime has 13 laws[11] and 7 Decrees[12].

The Ministry of Information Technology and Communications – MINTIC worked on a Government Online strategy from 2010 till 2014 and currently is implemented a second version from 2015 till 2018. It is called "Life Digital Plan 2.0" with the aim to "*give the country a technological leap by the massification of the Internet and the development of*

[10] For further information look at: http://www.uniandes.edu.co/component/content/article/656-about-uniandes viewed on 01 May 2016.

[11] Law 527 of 1999, Law 599 of 2000, Law 679 de 2001, Law 962 of 2005, Law 1150 of 2007, Law 1266 of 2008, Law 1273 of 2009, Law 1341 of 2009, Law 1437 of 20011, Law 1480 of 2011, Law 1581 of 2012, Law 1623 of 2013, Law 1721 of 2014.

[12] Decree 2364 of 2012, Decree 2609 of 2012, Decree 2693 of 2012, Decree 1377 of 2013, Decree 1510 of 2013, Decree 1510 of 2013, Decree 333 of 2014.

the national digital ecosystem."[13] MINTIC has done an efficient job of enhancing the citizens' access to Internet, as evidenced by the fact that connections have been triplicated during the last years.

Following the Global Cyber security index & cyber-wellness Profile Report – GCI in 2015, Colombia was classified in the Global Rank number 9 with an index of 0.588; the highest level was assigned to the United States with a value of 0.824. The GCI reflects the level of a state commitment in five areas: legal, technical, organizational efforts, capacity building and international cooperation but does not seek to determine the efficacy or success of a particular measure, rather the existence of national structures that promote cyber security [54]. Additionally, the GCI identified some aspects that might be improved in the country, for instances: Colombia doesn't have any educational program for raising Cyber security awareness and the government doesn't follow any international standard in cyber security. The educational and training component of the NCSS must be realised.

Although Colombia's government has worked in several aspects related to cyber security, there are many aspects that require an active intervention of the state. In 2014, OAS assessed Colombia's government, with the objective to advance cyber policies at national level and to map the current status of the country in regard to cyber security. Although part of this analysis is confidential some of the results that were published are: To update the CONPES-3701 and modify the way of Colombia approach the cyber security from the strategy part; to distribute the responsibilities equitably among stakeholders principally from the public side; to generate cyber-capabilities in cyber security and cyber defence, and to improve the international cooperation [9].

Colombia has advanced in the cyber security field. Organizational capacity was improved at all levels and responsibilities were assigned to some stakeholders. The existence of national guidelines, CERTs in critical sectors, legal framework and projects developed by different ministers are the meaningful results of the modest National Policy in the field. However, the created organizations don't have enough resources to do their job efficiently [9] The lack of trained people, enough resources and technological infrastructure; are the most critical factors that currently affect cyber security status in the country. One factor, which has been marked by several cyber security experts and organizations is the out-dated National Cyber Security Policy as well as that there is no significant advance in the identification, classification and categorization of the Critical Infrastructure and their dependencies either. Working on the maturity level of the existing agencies should be a good way to start the improvement of their cyber security present condition**.**

5.1.3 Vision, Scope and Objectives – Phase 1.4

To establish aims, scope and vision of a NCSS is considered as an intersectoral job and highly affected by the political will. This works proposes a set of aims applying the theoretical contributions developed in the chapters above that should be considered in the next Colombian NCSS. The scope and vision are not proposed by this research nonetheless according to the Colombian political organisation, these have to be applied till 2019 that corresponds to the presidential period and it depends of external factors as economic resources and political will.

Proposal aims according to internal priorities and national needs:

- Strengthen the capacities of the institutions created by the CONPES 3701 at the national levels;

[13] For additional information look at: http://www.mintic.gov.co/portal/604/w3-article-1971.html, viewed on 01 May 2016.

- To reinforce the legal framework for combating cybercrimes;
- Develop and implement a cyber security educational strategy;
- Work on strategies to enhance national and international cooperation, collaboration and coordination;
- Identify, prioritise and categorise the Colombian CIs.

5.1.4 Colombian Stakeholders for the formulation of NCSS – Phase 2.1

The stakeholders who could be called to participate in the development of a new Colombian NCSS are categorized in the Table 12 according to the developed guidelines and the comparison of the selected countries:

Table 12. Colombian Stakeholders.

Sector	Possible Representatives
Public Sector	• National Planning Department; • Ministry of Interior; • Ministry of Justice; • Ministry of Foreign Affairs; • Ministry of National Defence (National CERT, CCOC, Armed Forces, Intelligence); • Ministry of Education; • Ministry of IT and Communications; • Ministry of National Treasury; • National Protection Unit (UNP) - Intelligence Services.
Private Sector	To identify private stakeholders who should participate in the formulation of Colombian NCSS is a demanding work, due to the lack of information and a prior governmental identification. However, certain criteria could be considered for instance: in line with the National Statistics Department the Colombian ISP with major participation at national level are[14]: • Comunicacion Celular SA Comcel S.A; • Colombia Telecomunicaciones S.A E.S.P; • Colombia Movil S.A E.S.P; • UNE EPM Telecomunicaciones S.A E.S.P (DANE, 2015). Besides to consider companies as ECOPETROL.SA, which is an oil company that in 2014 it had the biggest operating income in Colombia with $57.454.644.360.000 Colombian Pesos, follows by TERPEL.SA with $12.709.766.540.000 Colombian Pesos. Additionally, the Colombian policymakers should consider organisations that represent SMEs. However, due to the large number of companies that are part of this group approximately 2.500.000 is recommendable to involve organisations that represent them, such as FENALCO[15].

[14] For further information look at: http://www.dane.gov.co/index.php/eng/, view on 15 April 2016.

[15] For further information look at: http://www.fenalco.com.co, view on 15 May 2016.

	Colombia has 8 CERTs registered in FIRST[16] organisation, although 3 of them represent governmental institutions that were taking in consideration above, others 5 represent different sectors, for instance: CSIRT OLIMPIA from Colpatria Group in representation of banking sector.
Representatives from the Academia	According to the Minister of Education the best Colombian universities in 2015 were[17]: • Universidad de los Andes; • Universidad Nacional de Colombia; • Colegio Mayor de Nuestra Señora del Rosario; • Universidad de la Sabana; • Universidad Eafit. These could be called to collaborate in addition to educative institutions, think tanks and research centers recognised for their interests in the cyber security area.
Civil Society (Citizens)	The Colombian population in 2016 is 48.680.620[18], so is recommendable to select organisations and/or associations to do this role within the development of NCSS, it is the case of ACUI (Asociacion Colombiana de Usuarios de Internet / Colombian Association of Internet Users). To a major participation social leader can be considered.
International Community	The Colombian government have required an official collaboration of the OAS to improve the cyber security at national level. Furthermore, the OECD guidelines are considered into the development and implementation of national policies in order to fulfil the minimum requirements to Colombia for being part of it. To engage international non- governmental experts or organisations is recommendable.

Although the CONPES-3701 ordered the CI identification, prioritisation and categorisation, after almost 5 years this process still in progress (OAS, 2014), it brings an additional complication about who should be call to collaborate in the new development of a NCSS at least from the private sector. Moreover, the national CERT do have the enough maturity and capacity to gather the principal private stakeholders [9]. A possible solution is to bring the companies that have a major representation taking into consideration the economical, social influence or geographic influence, direct dependencies on other infrastructures, etc.

To sum up, to select the appropriate stakeholders represents some difficulty in the Colombian case, which can be accomplished only with access to official information and participation of different agencies. At this point records and existing information are considered confidential.

[16] For further information look at: https://www.first.org/members/map#CO, view on 15 May 2016.

[17] For further information look at: http://www.mineducacion.gov.co/cvn/1665/w3-article-351855.html, view on 15 May 2016.

[18] For further information look at: http://www.dane.gov.co, view on 15 May 2016.

Additional Considerations:

The Colombian stakeholders should establish a secure information channel among them that can be use during the formulation of the NCSS *(Phase 2.2).* This research recommends that it could be in charge of the National CERT, because this institution is commonly responsible of leads collaborative activities at national level. Therefore, the ColCERT have means, protocols for multi-stakeholders activities and secure storage for gathering information through the development process.

Currently, Colombia does not count with a National Risk Assessment *(Phase 2.3)* that allows determining what risks and threats at national level are and how these could impact to the state. It is highly recommendable to develop this assessment for Colombia; it would help to stakeholders to improve the level of cyber security through more efficient measures and protocols based on actual threats and risks. Moreover, the result of it would help to select and prioritise aims as well as to establish the scope and limitations that would cover the NCSS.

The organisations responsible to lead the development of NCSS in Colombia are: the National Planning Department; the Ministry of National Defence, and the Ministry of IT and Communications. They should propose a working plan to the formulation of the NCSS *(Phase 2.4)*, it has to be shared with the stakeholders and adjusted according to the stakeholders' requirements. It is also recommendable to considered the proposal guidelines and the KPI related with this phase (Figure 9. Mix Approach for the development of NCSS and Table 10. KPI No 4: Working Plan).

5.2 Recommendations in Regard to the Colombian Case

The development of NCSS is a process that requires the multi-stakeholders collaboration and cooperation. Hence, it is not appropriate to apply the entire proposal guidelines without the intervention of at least some of them. In spite of this, an approximate study suggests recommendations that could be included into the next NCSS of Colombia *(Phase 3.1 and 4.1)*, whose issue is anticipated in 2016:

- The Intersectorial Commission is in charge of cyber security' strategic vision, and also to establish political guidelines for the management of the technological infrastructure does not cover the responsibilities of a national cyber security agency or similar organisation. Currently in Colombia a centralized high national agency, to lead all issues related to cyber security is missing. This organisation would work as a national coordinator with enough authority and resources to supervise stakeholders, ensure budget distribution, lead national risk assessment, etc.;
- In spite of earlier Colombian policy efforts to create a basic national structure, the maturity level of these organisations is low, mainly due to lack of resources (human, economic, facilities, and infrastructure). The ColCERT and CCOC have to focus on building capacity; resources should be assigned to these organisations but first of all the responsibilities and roles must be clearly defined, both agencies were created under the ministry of defence with overlapped functions. In the case of the CCP in charge of facing cybercrime at national level, the achievements have been better; they count with a considerable number of trained people, facilities and economic resources. However, the exponential growth of cybercrime and related matters, requires an increase of the state capacity to manage and operate;
- Although the Colombian government argue that it has improved the legal framework about and related to cyber security, it the legislation does not fully connect with concrete cases. The country requires laws and regulations on data retention and should

also update the existing ones regarding the commercial use of digital information, CIs' management, digital evidence, etc. The least costly solution could be the adaptation, amendment or review of the existing laws. In addition, public employees from the jurisdictional branch, prosecutors and court officials must be empowered with training and assign the means to support the whole system in an effective manner;

- The identification, prioritisation and categorisation of the CI are urgent. It would allow concentrating all kind of efforts; economic, human, technical and organisational on what is really important; it also helps to prioritise resources and formulate assertive strategies. Then, protection of these vital infrastructures would be coordinated and systematic;
- With help from other instances, at least with the participation of the Ministry of Education, the government should promote awareness, education and training in the area of cyber security. It may include interventions at different levels of education from the primary schools on basic skills of cyber security issues, and advanced awareness to postgraduate studies, together with specialized and continuous education programmes. Moreover, the ministry must associate with the different sectors to promote and support the research and innovation in this field. Incentives should be actually provided, rather than relying on issuing public policy documents alone.

On April 11, a new NCSS of Colombia was released under the name CONPES 3850. It was available to the public and published online at end of April. Consequently, it is not included as document or reference in this research. The new NCSS of Colombia matches the recommendations of the present study; in particular, on the areas in which the country should improve and the suggestions listed above.

6 Conclusions

Cyber security protects the lifestyle and general wellbeing in an interconnected age where virtually all information is processed by digital technologies. Not only businesses migrate to virtual environments, but also social interaction of all sorts and even the provision of public services such as in the case of e-governance. To face the transformative challenges that technology advancement imposes on society, governments have taken technical, economic, political and organisational steps, reflected in national strategies or similar documents. These are complex tools public policy tools that require expertise, resources and guidelines for their development and effective, rational implementation.

The outcome of this study resulted on one hand, in a set of working tools with contributions of significance to theory and practice. The first achieved to advance the terminology in the field and presented as a solution to the first research question on 12 guidelines divided into phases, that are adaptable and transferable. These established the considerations required to complete a systematic process of NCSS development. Additionally, and drawing from the information collected, a Key Performance Indicators self-assessment list was proposed in terms of 5 categories to affirm the benefits of measuring parameters, and a format for 6 essential components to be included in NCSSs could be put together. These last may strengthen cooperation if used to disseminate a common understanding in communications across instances as well. On the other hand, the partial application that could be performed on the basis of these theoretical perspectives, illustrates sufficiently the process, as it was required to address the second research question. However, the main limitations of the study also became apparent at this stage. Namely, the constraints that arose due to the lack of information that was classified then or does not exist, on areas that require precision such as the identification of critical infrastructures, risk and needs assessments that would only be possible if to consult all stakeholders could have been possible, etc. If proceeding without this last input (the stakeholders involvement or the collaboration factor), continuing the process would contradict the spirit of the guidelines.

Nonetheless, the case study afforded practical suggestions that could improve the cyber security status of Colombia: The country needs to clarify who are the stakeholders and their roles and responsibilities; the government should focus on building capacity of the agencies created by the CONPES 3701; the legislator should reinforce and update the current legal framework; the Colombian CIs must be undoubtedly identified, categorised and prioritised; and, serious campaigns have to promote awareness, education and training in cyber security areas across curricula from the early primary school to the tertiary educational levels.

Although generalisation does not work as a stand-alone solution for the development of NCSS the final objectives, threats and key actions lines can be grouped into general categories that follow accepted principles and common perspectives. All countries want to combat industrial cyber espionage; prevent cyber terrorism and cyber attacks; protect privacy and confidentiality, availability and integrity of information; and combat cybercrime. The means to achieve these objectives also shared an increase of awareness, education and training; creation and/or strengthening of legal frameworks; raising resilience of the services and network systems; protection of the CIs and vital networks, etc. Multi-stakeholders' collaboration, cooperation and coordination are presented as key aspects for the consolidation of better cyber security activities at the global level. To reach a mutual understanding and consent on the terminology outside of the academic environment is a demanding job of serious implications. Using the same language is not achieved with the issuing of a document. Working on the much desired common understanding of cyber security and related terms would in turn enhance the quality and transparency of cyber security agreements by stakeholders, it does not simply constitute and advance the theoretical grounding of concepts.

The avenues for future research are promising: these concepts could be applied to more case studies or scenarios and collect data for analysis and verification on impact and efficiency, using mixed methods. National strategies have political, economic, social and organisational components that should be observed and scrutinized separately, so to count with more experts and study groups that could contribute to this line of research, which is needed too.

The development of NCSS strategies is a multi-stakeholder process that involves national and international factors. Moreover, it is highly influenced by the will and interests of the participants, which are, understandably, diverse and may appear contradictory. Theses special characteristics cannot be captured and problematized in one academic paper only. Additionally, there is an unavoidable complication in research concerning public order and states' security: crucial information cannot be disclosed to the public. This shortage of information applies to the development of NCSSs. In some Countries the documentation of such processes is disallowed, and when records are kept, only final texts are published. It is an inefficient state practice that studies must be conducted later on. The validation of this proposal requires time; to know the actual depth and breadth of impact of a NCSS implementation must begin. Some predictions could potentially be elaborated on, but this is a task for further research and a professional responsibility that will follow.

7 References

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

[2] R. O. Mason, "Four Ethical Issues of the Information Age," *Gdrc.Org*. 1986.

[3] E. Luiijf, K. Besseling, and P. De Graaf, "Nineteen national cyber security strategies," *International journal of critical …*, no. July 2015. pp. 2–31, 2013.

[4] C. Czosseck, R. Ottis, and A.-M. Taliharm, "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *Case Stud. Inf. Warf. Secur. Res. Teach. Students*, p. 72, 2013.

[5] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Secur. Priv.*, vol. IEEE, 9(3), pp. 49–51, 2011.

[6] Z. Fang, "E-government in digital era: concept, practice, and development," *Int. J. Comput. Internet …*, vol. 10, no. 2, pp. 1–22, 2002.

[7] S. R. Chabinsky, "Cybersecurity Strategy : A Primer for Policy Makers and Those on the Front Line," *J. Natl. Secur. Law Policy*, vol. 4, no. 27, pp. 27–39, 2010.

[8] A. Klimburg(Ed)., *NationalCyberSecurityFrameworkManual.pdf*. 2012.

[9] OAS, "International Cyber Security Technical Assistance Mission Colombia, Recommendations and Observations," Bogota, Cundinamarca., 2015.

[10] A. S. Lee, "Challenges to qualitative researchers in information systems.," *Qual. Res. IS Issues trends*, pp. 240–270, 2001.

[11] A. C. Cooper and D. E. Schendel, "Strategy Determination in Manufacturing Firms: Concepts and Research Findings," *Grad. Sch. Ind. Adm. Purdue Univ.*, 1971.

[12] D. E. Schendel and K. J. Hatten, "Business Policy or Strategic Management: A Broader View for an Emerging Discipline," *Acad. Manag. Natl. Meet.*, 1972.

[13] Government of Jamaica, *National Cyber Security Strategy*. 2015.

[14] Netherlands, "National Cyber Security Strategy 2," 2013.

[15] Australian Government - Attorney General's Department, "Cyber Security Definition," *Cyber Security*, 2016. [Online]. Available: https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx. [Accessed: 01-May-2016].

[16] P. M. Shane, "Cybersecurity Policy as if 'Ordinary Citizens' mattered: The case for public participation in cyber policy making," *Isjlp*, vol. 8, no. 2, pp. 433–462, 2012.

[17] ITU, "Definition of Cybersecurity," *Cyber Security*, 2016. [Online]. Available: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx. [Accessed: 01-May-2016].

[18] The Republic of Colombia, *Policy Guidelines on Cybersecurity and Cyberdefense*. 2011.

[19] J. R. Lindsay, "Stuxnet and the limits of cyber warfare," *Secur. Stud.*, vol. 3, pp. 365–404, 2013.

[20] U. Mummert, A. Mummert, "Success Factors for Development Strategies : Adding

Structure to the Glut," *Cent. Appl. Int. Financ. Dev.*, vol. 2, no. ISSN 2191-4850, pp. 1–45, 2011.

[21] X. Zhuo, B. Wellman, and J. Yu, "Egypt: The First Internet Revolt?," *Bol. do Tempo Present. ISSN 1981-3384*, no. 1919, pp. 1–10, 2015.

[22] Kalathil S and Boas TC, "The Internet and state control in authoritarian regimes: China, Cuba and the counterrevolution," *First Monday*, vol. 6, no. 8, pp. 1–18, 2001.

[23] A. Friedman, "Economic and Policy Frameworks for Cybersecurity Risks," no. Center for Technology Innovation at Brookings, pp. 1–23, 2011.

[24] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, "The economic impact of cyber-attacks," *Congr. Res. Serv.*, no. Library of Congress, 2004.

[25] T. Moore, "The economics of cybersecurity: Principles and policy options," *Int. J. Crit. Infrastruct. Prot.*, vol. 3, no. 3–4, pp. 103–117, 2010.

[26] R. Deibert, "Towards a cyber security strategy for global civil society?," *Glob. Inf. Soc. Watch*, pp. 23–26, 2011.

[27] B. Dupont, "The proliferation of cyber security strategies and their implications for privacy The compressed chronology of cybersecurity strategies," *Canada Res. chair Secur. Technol.*, no. February, pp. 1–11, 2013.

[28] A. Steurer, R., Martinuzzi, "Towards a new pattern of strategy formulation in the public sector: first experiences with national strategies for sustainable development in Europe," *Environ. Plan. C Gov. Policy*, vol. 23, pp. 455–472, 2005.

[29] H. Mintzberg, "the Design School: Reconsidering the Basic Premises of Strategic Management.," *Strateg. Manag. J.*, vol. 11, no. 3, pp. 171–195, 1990.

[30] T. Poister and D. Streib, "Strategic management in the public sector: concepts, models, and processes," *Public Product. Manag. Rev.*, vol. 22, no. 3, pp. 308–325, 1999.

[31] A. Kronz, "Managing of process key performance indicators as part of the aris methodology," *Corp. Perform. Manag.*, no. Springer Berlin Heidelberg, pp. 31–44, 2006.

[32] W. Frederick, *The ITU National Cybersecurity Strategy Guide*, no. 1. 2012.

[33] OECD, "Digital Security Risk Management for Economic and Social Prosperity," *OECD Recomm. Companion Doc.*, OECD Publishing, 2015.

[34] N. Falessi, R. Gavrila, M. Klejnstrup, and K. Moulinos, "National Cyber Security Strategies. Practical Guide on Development and Execution," *Eur. Netw. Inf. Secur. Agency*, no. December, p. 15, 2012.

[35] ENISA, *An evaluation Framework for National Cyber Security Strategies*. 2014.

[36] M. N. Schmitt, *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

[37] C. F. Goodwin and J. P. Nicholas, "Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation," no. October, 2013.

[38] K. Giles and W. Hagestad, "Divided by a Common Language : Cyber Definitions in

Chinese , Russian and English," *5th Int. Conf. Cyber Confl.*, pp. 413–429, 2013.

[39] G. III, K. Audrey, R. Karl, and Y. Valery, "Critical Terminology Critical Terminology Foundations 2," *EastWest Inst. Inf. Secur. Inst. Moscow State Univ.*, vol. 2, 2014.

[40] Rauscher, F. Karl, and V. Yaschenko, "Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations," *New York, USA EastWest Inst.*, vol. 1, pp. 1–40, 2011.

[41] D. Craigen, N. Diakun-thibault, R. Purse, D. Craigen, and N. Diakun-thibault, "Defining Cybersecurity," *Technol. Innov. Manag. Rev.*, pp. 4–10, 2014.

[42] Republic of Turkey, "National Cyber Security Strategy and 2013-2014 Action Plan," 2013.

[43] Hungary, *National Cyber Security Strategy of Hungary*. 2013.

[44] The Czech Republic, "National Cyber Security Strategy of The Czech Republic for the Period from 2015 to 2020," 2015.

[45] Austria, "Austrian Cyber Security Strategy," 2013.

[46] The United States, "National Security Strategy," 2015.

[47] http://www.nisc.go.jp/, "Cybersecurity Strategy," 2013.

[48] Bailes, A. JK, and K. Þ. Ólafsson, "Developments in Icelandic Security Policy," *Stjórnmál og Stjórnsýsla*, vol. 2, 2014.

[49] Iceland, "Icelandic National Cyber Security Strategy 2015–2026," April, 2015.

[50] France, "French National Strategy Digital Security Strategy," pp. 1–40, 2015.

[51] The Slovak Republic, "Cyber Security Concept of the Slovak Republic for 2015 - 2020," 2015.

[52] OAS and Trend Micro, "Report on Cybersecurity and Critical Infrastructure in the Americas," 2015.

[53] Newmeyer and K. P., "National Cybersecurty Institute Journal," *Natl. Cybersecurty Inst. J.*, vol. 1, no. 3, 2015.

[54] ITU, "Global Cyber security index & cyber-wellness Profile Report," 2015.

Appendix

I. Online Questionnaire

- How cyber security should be defined?
- Should a country design a cyber security strategy?
- Who should be called to participate in the formulation of a cyber security strategy for a country?
- What standards are used to develop national cyber security strategies?
- What evaluation methods can determine the effectiveness of a cyber security strategy, if any?
- What problems and obstacles could arise in the formulation of a cyber security strategy?
- What is your country of origin?
- What is your current occupation?
- What is your age group?

II. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Yuri Andrea Pinto Rojas**,

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

Development of National Cyber Security Strategies (NCSSs), and an Application of Perspective to the Colombian Case,

Supervised by Maria Claudia Solarte Vasquez and Raimundas Matulevicius,

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**