European Studies, 10th Semester
Master Thesis

Aalborg University
July 31st , 2015

The European Union Cyber Security Strategy
Decision Making and Policy Harmonization in EU

Author
Ana Mihaela ANTON

Supervisor
Elijah Nyaga MUNYI

Keystrokes: 153 000

Acknowledgement

In the process of writing this thesis many have contributed and helped me along the way, and I would like to acknowledge these efforts.

I would like to express my gratitude to my supervisor, Mr. Elijah Nyaga Munyi, for his constructive guidance through the process of writing this thesis and valuable advice along the way. I very much appreciate your time.

I would also like to give special thanks to my sister and my boyfriend for their positive criticism and support.

Furthermore I would like to thank my parents and friends who have helped me with large and small things along the thesis writing process.

ABSTRACT

Cyberspace has become part of our daily life as the majority of activities are nowadays connected with the high-tech industry. In addition, societies have become digitalized and cyberspace has become a new factor of interest in world politics.

As the use of Internet is expanding exponentially, influencing all actors within our society, it has become clear that the ease of access to data brings together security issues. Cyber-attacks on public and private actors are reported daily and this increasing number of attacks have economic and social consequences within a state. These has made officials acknowledge the need to protect public and private networks.

However, it is intriguing that given the impact that cyber-attacks could have and the fact that in the last years, at European Union level efforts have been put towards promoting cyber security, it is the case that until now the European Union does not have a common approach toward accomplishing this goal.

The purpose of this paper is to examine the ongoing process of approval of the Network and Information Security Directive at European Union level. The Directive proposes a common framework in handling cyber security and it is supposed to create a collaboration network within the Member States. Such measures will positively affect both citizens and business and will create a standardization in the field of cyber security at European level.

Given the fact that the proposed Directive is still under negotiation, I will undertake an investigation in identifying the elements that might hinder progress in the field.

The following investigation will target decision making and policy harmonization at European level and will identify the major influences that can be connected to the lack of visible progress in the field of cyber security.

ABREVIATIONS LIST

CA	Competent Authority
CERT	Computer Emergency Response Team
CSIRTs	Computer Security Incident Response Team
COREPER	Committee of Permanent Representatives
EC	European Commission
ECJ	European Court of Justice
EC3	European Cybercrime Centre
EIB	European Investment Bank
ENISA	European Network and Information Security Agency
ENPI	European Neighbourhood Policy Instrument
EP	European Parliament
EU	European Union
EUR	Euro
TFEs	Full Time Equivalents
ICT	Information and communications technology
IMCO	Internal Market Committee
IT	Information technology
LI	Liberal intergovernmentalism
MSs	Member States
NCA	National Competent Authority
NIS	Network and Information Security
OECD	Organisation for Economic Co-operation and Development
SEA	Single European Act
SME	Small and Medium Enterprises
sTESTA	Secure Trans European Services for Telematics between Administrations
TTE	Transport Telecommunications and Energy
UK	United Kingdom
QMV	Qualified majority voting
WP TELE	Working Group on Telecommunications and the Information Society

TABLE of CONTENTS

I. Introduction

"Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly"
(Cyber security Strategy of the European Union, 2013: 2).

The invention of the computer in the 60's and the appearance of the World Wide Web in 1991 and its introduction to the large audience has changed the way we communicate, work and interact and has altogether transformed societies.

Nowadays most of the societies are connected to what is called cyberspace; without a generally accepted definition of the term, given the fact that it covers everything from software, hardware, the Internet, information, cables, servers, computers, but also interactions between individuals, states, companies and cultures.

This transmission of data has made societies more efficient, as the digitalization reached all parts of modern societies; computers are being used for everything from teaching/learning, paying bills, transferring money, storing critical information, flying airplanes and drones to communication between the state and the public. Furthermore, digital communities have also become a new factor within world politics and therefore a new power element within the balance of sovereignty (Barett et al, 2011).

The use of the Internet and the amount of data available is increasing by the day and digitalization, characterized by the borderless nature and global accessibility of cyberspace has become a global common. In other words "*the vast amount of digitized information that travels across the electromagnetic spectrum is the 'payload' of cyber space and is available to anyone with the technical means, such as a computers or a smart phone, to gain access*" (Barett et al, 2011:37). This ease of access to data brings critical security issues.

Cyber security was first used by computer scientists in the early 1990s to underline a series of insecurities related to networked computers, but it moved beyond a mere technical conception

of computer security when advocates urged that threats arising from digital technologies could have devastating societal effects (Nissenbaum, 2005).

Over the last several years, the world has witnessed such security challenges. Attacks include the 2007 cyber-attack on Estonia, the 2008 attack on the state of Georgia, the Stuxnet virus from 2009 that attacked the Iranian nuclear program, and the actions undertaken by the hacker group "Anonymous" against companies such as Visa, MasterCard, PayPal, and Amazon over the Wikileaks scandal. Each attack illustrates the potential destructiveness within state actors and important institutions (Greathouse, 2014).

The extensive number of attacks in cyberspace has economic and social consequences, resulting in the acknowledgement of the importance of securing cyberspace by state actors and furthermore by the institutional developments worldwide.

President Obama has admitted cyber threats as a serious economic and national security challenge in the 21st century and acknowledged that how this will be handled will affect the economic prosperity of the United States. (White House, 2009). This logic can apply to any state, given the fact that more and more nations depend on information communication and technology.

Following the same line, the European Commission states that "*cyberspace should be protected from incidents, malicious activities and misuse*" (European Commission, Cyber security strategy, 2013:2).

Network and information systems are of great importance in facilitating movement of goods, services and people, principles that comes as the EU' foundation. Additionally, as the Internet is characterized by its global nature, such networks develop increased interconnectedness between EU's Member States. This can be translated in the risk of other Member States or overall the Union being affected by an incident that happened in one of them. Therefore, a well-functioning Internal Market comes in line with the need of stable and protected network and information systems. Given that, as shown above, these systems are interconnected, actions need to be taken at European level (European Commission, 2013c).

1.1. Preliminary knowledge

Over time, the EU has outlined cyberspace as a security issue and looking at the existing EU provisions in the field of cyber security, as a securitizing actor, the EU has put the issues of cyber security on the agenda through various policies.

In 2001, the European Commission outlined the importance of network and information security in a proposal for a European Policy Approach. Aiming at the development of a network and information security, a Strategy for a Secure Information Society was adopted in 2006.

In 2004 the European Network and Information Security Agency (ENISA) was established, which aims at creating a high level of network and information security across the EU.

Besides establishing programmes and implementing policies as to ensure network and information security, the European Union has also created institutions that take cyber security outside of normal politics. As it is pushed forward, "*the EU and the Member States need strong and effective legislation to tackle cybercrime*" (European Commission, 2013c: 9).

In this regard, the Council of Europe Convention on Cybercrime (2001) is the basis for the creation of a binding international treaty that is to be translated into national legislation by the signatory states[1] and few of the original signatory states have not ratified yet the Convention[2].

Established in January 2013 by the European Commission, the European Cybercrime Centre (EC3) represents an example of how cyber threats are securitized at the European level. Part of the European Police Office, this body is a focal actor in the fight against cyber-crime (European Commission, 2013c).

On 2nd February 2013, the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy published a strategy - "An Open, Safe and Secure Cyberspace" accompanied by a proposed Cyber Security Directive.

[1] Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.
[2] As per 09/06/2015: Greece, Ireland, Sweden, Canada, South Africa

According to the European Commission "*the cyber security strategy represents the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks. This is to further European values of freedom and democracy and ensure the digital economy can safely grow*", thus within the strategy, the proposed directive is a key component. (Commission, Press Release, 7 February 2013)

Taking part at the press conference that followed the publication of the EU's Cyber Security Strategy and the proposed Directive, Catherine Ashton, European Commission Vice President and High Representative of the European Union for Foreign Affairs and Security Policy, stressed the importance of measures in the cyberspace - "*At the heart of our policy is our firm belief that the protection of fundamental rights is as important in the virtual world as it is in the real world - we are united in Europe on this principle. For cyberspace to remain open and free, the same norms, principles, and values that we uphold offline must also apply online*" (Hammond, February 2013:3)

1.2. Problem presentation

As shown above, cyber security policy has been on the EU' agenda for many years now, but for some reasons the progress made in the field does not seem to come in line with the intensity of threats in the cyberspace.

The establishment of the European Network and Information Agency (ENISA) in 2004 in order to facilitate shared knowledge and improve "best practices" among Members States, together with other actions, such as the establishment of a Digital Agenda for Europe 2010 is part of the progress made insofar in the area of cyber security. More efforts in securing cyber space was undertaken in EU following the attacks on Estonia's public and private infrastructure.

The cyberspace offers meaningful opportunities for social development and economic growth, but at the same time, it poses the threat of insecurity thus presenting danger for state infrastructure, businesses and citizens. At the EU level this presumption transfers in factual data, as in 2013 business leaders and governments officials consider cyber security risks of greater impact that terrorism risks (World Economic Forum, 2013).

In order to respond to these concerns, EU Member States have tackled this issue at national level, by elaborating legislation or strategies. However, as shown by ENISA (2014), not all Member States (MSs) have National Strategies in place in relation with cyber security and the threats that arise from this sphere.

Given the issues that cyber security poses to states and the fact that EU harmonization in matters of cyber security has not yet been assured, the aim of this paper is to investigate the motives behind the moderate measures taken by the EU. This is translated in an investigation regarding the process of adopting the Cyber Security Directive, published by the European Commission in 2013.

Taking into consideration the most obvious connotations of the EU's actions in regards with cyber security – the Cyber Security Strategy put forward by the European Commission, as well as its lack of action - the on-going negotiations in adopting the Commission's Proposed Directive, that is the means of achieving the Strategy's points, I have identified several elements that interacts within the EU policy making process.

- **The EU's institutions role**

As a sui generis institution, the European Union proves to be a challenge within the security area. Even if it is an actor in international relations, with even more decision making power since the Lisbon Treaty of 2009 which codified the EU's legal personality, cooperation within the security area is essentially intergovernmental. Major decisions of the European Council and the Council of the European Union are taken either by consensus or by unanimity, therefore it can be stated that national narratives impede the emergence of a true common vision. On the other hand, it is believed that most of the decision making within the Union takes place at supranational level. Therefore an investigation of the importance of the EU institutions in the process of approval of the Directive has to be undertaken.

- **Member states interests**

In a progress report of the EU Council it is stated that some member states incline towards a more voluntary approach than a legislative one as an option to tackle the problem of the proposed NIS Directive. At the same time, countries like UK and Germany are pressing for measures in line with their own legislation. Such elements can influence the debate around EU's position in the sector.

- **Industry stakeholders pressure**

Besides their influence in policy making, as per example lobby within the EU Commission, stakeholders exercise pressure also on national government level.

Within the cyber security issue, the industry points out the risk of damage to reputation and impact of share price and customer loyalty in regards with the issue of mandatory reporting that Commission's Proposal requires upon approval. Furthermore, it is added that in other parts of the world a voluntary and flexible approach is attempted and such mandatory standards from EU "*might create inconsistencies for companies whose operations span several jurisdictions, as is usually the case with many online services*" (The EU Council progress report, 2013:8).

The above illustrated point of influence in the decision making process will not be treated as to find a sole response, but quite in opposition. They are intended to lay down a proper empirical data that can support the analysis in order to answer the following question:

What could be the nature of the holdbacks in agreeing on a common cyber security policy in the EU?

The answer to this question will translate first into an investigation of the theoretical framework attributed to decision making within the EU, following an investigation into the process of adopting the NIS Directive. This will support the analysis by establishing from what perspective one can look into the decision making process regarding within the field of cyber security.

1.3. Synopsis

The project is divided into six chapters, as illustrated in Fig 1. Project Structure.

The **first chapter** is defined by the Introduction and the Problem formulation and aims at introducing to the reader the aspects discussed in this paper. Following, a presentation of the thesis will be outlined.

The **2nd chapter** is concerned with explaining the theories identified to fit the decision making process with EU and to discuss their applicability in this case.

Chapter three will represent the Methodology part. Within this chapter, I will define the ontology and epistemology taken within the research and analysis of the problem at hand. Following, data and sources will be presented and within the last part of the chapter, a theoretical discussion will be brought in order to review the chosen theories and identify limitations.

Chapter four is constituted by the empirical data, namely the case study, gathered and employed to establish a clear context for the thesis. The case study illustrated the NIS Directive and the on-going negotiation for its approval.

The fifth chapter, enclosing the analysis, will come to offer an answer to the problem under investigation by identifying how one can see the process of approval of a cyber security legal framework at EU level and the holdbacks within, thus determine the theoretical perspective/perspectives that explain the changes in the Directive.

Last, the **sixth chapter** will draw up the conclusions on the margin of the findings illustrated by the paper.

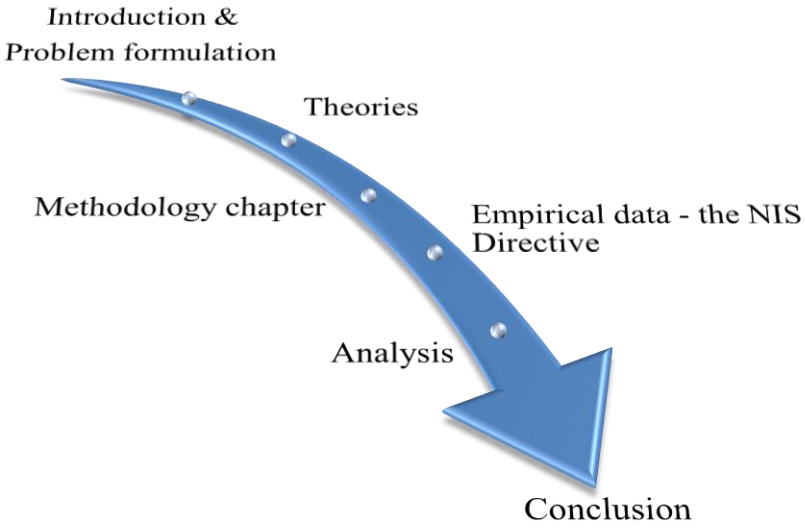

Figure 1 Project Structure

II. Theories

The theoretical framework chosen has taken into consideration the most prominent lines of thought when it comes to decision making in the EU. Therefore this chapter will tackle liberal intergovernmentalism, the new institutionalism and constructivism approach of decision making. Moreover, the theory on salience is presented as the intensity on interest that is attached to an issue. In the last part of the chapter, theoretical frameworks for policy making are exposed. The chapter ends with a discussion regarding the chosen theories and how they fit the problem under investigation.

Theories abstract

Developed by Andrew Moravcsik in the 1990s, liberal intergovernmentalism has been labelled as the most elaborate version of intergovernmentalism (Moravcsik 1993, 1998). Moravcsik has put forward a new way of thinking about the European integration by connecting a liberal theory of state preferences and a neoliberal theory of international interdependence and institutions to earlier approaches, predominantly of the realist line of thought.

Summing his theory, Moravcsik (1998: 4) argues

> *"that a tripartite explanation of integration – economic interests, relative power, credible commitments – accounts for the form, substance, and timing of major steps toward European integration".*

As put forward by Thomas (2008:7), "*institutionalist theories of European integration and governance treat the EU as a community of states whose rules and supranational organizations exert a significant impact on policy outcomes*".

***

Citing the most prominent theoreticians in their fields, Thomas (2008) realizes an overview of the different versions of institutionalism. Armstrong & Butler 1998, Sandholtz & Stone-Sweet 1998 emphasize the role of "*EU's supranational organizations and transnational policy*

entrepreneurs" (Thomas, 2008:8). On the other hand, theoreticians as Tsebelis 1994, Garett and Tsebelis 1996 underline the importance of formal rules, like the EU treaties. Additionally, others emphasize "*the behavioural impact of standards of appropriateness established by the community's normative and policy commitments*" and push forward a version of Institutionalism called Normative Institutionalism. (Thomas, 2008:8)

***

The constructivist theories of international relations and European governance sketch the EU as an integrated political community that transforms without doubt the policy preferences of the Member States. Such transformation is obtained though communication of normative reasons that should be taken into account by the MSs in reconsidering their identities and interests. Such communications are more likely happen within the Council's working groups or the Committee of Permanent Representatives.

2.1. Liberal intergovernmentalism

Liberal intergovernmentalism (LI) was first introduced by Moravcsik (1993) as a response to the criticisms brought to neo-functionalism in trying to explain the European Union integration and the common policies at the EU level. Criticisms to neo-functionalism point toward the idea that the EU should be seen as an international regime for policy-coordination. According to Moravcsik (1993) such coordination within the European Community may be explained by examining the national preferences formation and the strategic interaction between governments within.

A first attempt to illustrate such coordination within the EC was pushed forward by Moravcsik (1991) in an approach that tried to theorize interstate bargaining and institutional compliance – intergovernmental institutionalism. However, LI moves forward and besides refining the theory of intergovernmental institutionalism it adds the theory on national preference formation set within the liberal theories of international interdependence (Moravcsik, 1991).

In his attempt to explain policy making in the EU, Moravcsik puts at the core of liberal intergovernmentalism three essential elements. First, the assumption of rational state behaviour is accepted**,** followed by a liberal theory of national preference formation and lastly an intergovernmentalist analysis of interstate negotiations. (Schimmelfennig, 2001)

The assumption of rational state behaviour

This provides a general framework of analysis for the EU integration, therefore decision making. Within this theory, the primary determinants of national preferences are the costs and benefits of economic interdependence. Moreover, "*the relative intensity of national preferences, the existence of alternative coalition and the opportunity for issue linkages provide the basis for an intergovernmental analysis of the resolution of distributional conflicts among governments*" (Moravcsik, 1993:480).

In making his argument, Moravcsik uses regime theory, as at any particular moment state action is assumed to be of a minimum rationality, respectively, it is directed towards achieving a set of clearly goals or objectives. This served to analyse the conditions under which governments delegate powers to international institutions.

Liberal theory of national preference formation

Accepting that "*governments evaluate alternative courses of action on the basis of a utility function*", the theoretician follows liberal theories of international relations that focus on state-society relations. In contrast with realist and neo-realist approaches that see states with fixed preferences for wealth, security or power, the side explored by Moravcsik views foreign policy goals variable, in relation with the shifting of pressure for domestic social groups. (Moravcsik, 1993:481)

Therefore, national interests emerge through a domestic clash of societal groups that compete for political influence and policy making. Thus in Moravcsik' view[3] understanding of domestic politics becomes a precondition in analysing the strategic interaction among states.

Taking such into consideration, the model of rational state behaviour based on domestically constrained preferences according to Moravcsik (1993) implies that international cooperation

[3] Moravcsik, 1991, 1992b

or if the case, conflict can be modelled as a two stage process: firstly states define a set of interests, secondly they bargain among them in pursuing and in realizing those interests.

Intergovernmentalist analysis of interstate negotiations

According to all presented above, the interaction between preferences and strategic opportunities within national governments and the interstate interactions of preferences and strategic opportunities within the EC political system shapes the foreign policy behaviour of states. (Moravcsik, 1993)

Thus, liberal intergovernmentalism "*integrates within a single framework two types of general international relations theory often seen as contradictory: a liberal theory of national preference formation and an intergovernmentalist analysis of interstate bargaining and institutional creation*" (Moravcsik 1993: 482)

Liberal intergovernmentalism assumes "*European integration…as a series of rational choices made by national leaders*"[4] in response to international interdependence. Thus, integration results from three steps that translate the stimulus created by international interdependence into collective institutional outcomes. Therefore, the process is the following: domestic formation of nation preferences, intergovernmental bargaining to substantive agreements and creation of institutions at supranational level in order to secure these agreements.

In respect with decision-making within the EU, liberal intergovernmentalism view outcomes determined by relative power, the formal decision-rule, utilitarian interest calculations and strategic rationality. Theoreticians take an ontological perspective characterized by identities and interests. Within decision-making of policies at EU level, the outcome is given by the preferences of societal actors and economic pressure groups, translated through the state to the national interests and positions of member states, which are then represented in negotiations. (Moravcsik, 1998)

On the other hand, critics (Pierson, 1996: Wallace et al, 1999) have raised the point that LI provides a framework for individual intergovernmental bargaining episodes and therefore fails to take into consideration the fact that some integration decisions are constrained by the

[4] Moravcsik, 1998, p 18

effects of previous integration decisions. Such position can be put in line with Haas spill overs within the neo-functionalist theory of regional integration.

2.2. New Institutionalism

Following the underlying assumption that institutions matter in the sense that political struggles are mediated by prevailing institutional arrangements, theoreticians have sought to explain the EU governance and decision-making with the broad lines of new institutionalism.

Institutions are looked upon as "*extending beyond the formal organs of government to include standard operating procedures, so - called soft law, norms and conventions of behaviour"* (Bulmer, 1993:355). Institutionalists agree that these features of international institutions shape the political behaviour. However, it is recognised that "*institutions do not generate political behaviour of their own accord; they should not be seen as the determinants of policy*" (Bulmer, 1993:355).

New institutionalism presents important insights and analytic tools for clarifying the role of institutions in EU policy making process, arguing that institutions are the source of political behaviour not just impartial bodies which have the role of transforming actors' preferences into policies.

The analysis undertaken by the New Institutionalism of the EU reveals that the EU's common institutions are often more than mere arbiters in the decision-making process, and those institutions have become key players in their own right (Peterson & Boomberg, 1999).

In its study of the European integration, Rosamond (2000) notes that the EU institutions are not just simple forums within which politics occurs, but they can offer framework within which actors can carry out a relatively higher amount of constructive sum deals. In other words they constitute the principal variables between actors (embodied as member states, stakeholders, civil society, etc.) preferences and the policy outputs.

Other theoreticians, such as North, take the perspective of institutions being a pressure for political action, as "*the institutions define (or at least constrain) the strategies that political*

actors adopt in pursuit of their interests" (Rosamond, 2000:116). Thus, Member States benefit from the functions of the EU' institutions.

Following the institutionalism way of thinking, Pierson goes beyond the simple benefit of the moment and argues that "*actors may be in a strong initial position, seek to maximize their interests and nevertheless carry out institutional and policy reforms that fundamentally transform their position in ways that are unanticipated or undesired*" (Pierson, 1996:126). In other words, actors - states may not be fully aware of the future implications and possible and/or unintended consequences of participating in institutional venues in begin of their cooperation within an institutional framework, as the EU institutions.

Furthermore, it is common tendency that after a while, national governments lose control over the institutions created originally to strengthen them, and consequently the EU develops according to its own integrative logic. Bulmer goes further, arguing that institutions do not represent only a mediator of the actors within them and do not merely reflect their interests. On the contrary, the institutions themselves shape the actors preferences and power by structuring the access of political forces to the political process, thus creating a kind of bias. (Bulmer, n/a)

Supporting such considerations, March and Olsen (1984) view institutions as setting of beliefs, knowledge, values and norms; a context with a pre-established ways of doing things and thus shaper of the behaviour of participating actors.

From this standpoint, it is useful to examine actual and potential effects of the institutionalization of an EU decision making. North suggests that cooperation becomes 'institutionalized' when "*individuals repeatedly interact, when they have a great deal of information about each other, and when small numbers characterize the group*"[5]. Thus, more exposed to the institutionalism influence are working groups formed for specific policies.

Within this theory, several sub-files can be distinguished, one of them being the normative institutionalism. Bulmer defines institutions as a sum of "*formal institutions, informal institutions and conventions, the norms and symbols embedded in them, and policy*

[5] North, D.C. (1990) Institutions, Institutional Change and Economic Performance, Cambridge and New York: Cambridge University Press, pp12

instruments and procedures", thus it includes also the less formalized arena of politics, culture of political institutions. Moreover, Normative Institutionalism points out that the EU's normative and policy commitments exert a behavioural impact on the participants to the decision making. (Bulmer, n/a:13)

2.3. The Constructivist approach

Same as institutionalists, constructivists agree that institutions matter in the sense of having a causal influence in international relations, however, the constructivist approach differ fundamentally from the institutionalism presented before in their view of how institutions matter.

The constructivist approach sees institutions as an inclusion of informal norms and intersubjective understandings besides the formal rules (Checkel, 1998). Moreover, constructivists postulate a more important role to institutions, which create actors and not only their motivations but also their preferences and identities.

As outlined by Pollack (2001), studying the European Union, many authors (Sandholtz, 1993; Risse, 1996; Jorgensen, 1997; Wind, 1997; Matlary, 1997; Lewis, 1998) argued that EU institutions shape, besides the individuals and Member States behaviour, also their preferences and identities. Moreover, Christensen et al. (1999) argue that the constructivist perspective can be a basis for understanding a broad range of social ontologies, as per example identity, community and collective intentionality.

Over the years, constructivist work focused on testing hypothesis about socialization, norm-diffusion and collective preference formation in the EU, thus putting forward new findings in what influences decision making in the EU.

In concordance with the constructivist approach, important socializing effects on actors are to be attached to EU institutions. In this understanding, the EU consists of a system of principles, rules and procedures that might have socializing effects on actors exposed to them.

These socializing effects go beyond instrumental adaptation and strategic calculation and include also the internalization of norms and rules into self-conceptions. (Risse & Wiener,

1999; Lewis, 2003) Explaining it differently, institutional and normative environments are to be considered causal variables that can transform actors, including the conception of self of the individuals and how they form their interests.

Following such assumptions, an extensive number of studies have been undertaken in order to understand the socializing role of the EU institutions in the sense of how continuous interaction between actors in a group influence their position in decision making process. Thus, research has been concentrated on professional group in the EU such as the Committee of Permanent Representatives (COREPER), European civil servants, members of interest groups (Shimmelfenning, 2001: Checkel, 2003; Lewis, 2005, 2008; Thomas, 2008).

Accordingly, one can conclude that following the above idea, actors involved in the decision making process are being somehow constrained to behave in accordance with the norms of the institution or the group within which they interact. Thus influencing the decision making process.

An advantage of this way of thinking is that "*issue complexity [...] seems to decrease in the fields where socialization occurs*" (Saurugger, 2013: 895). In other words, socialization has lowered the number of levels where "*reality is constructed*" (Saurugger, 2013: 895), solving thus a major challenge of research collection in European integration study.

However, a major controversy is to be answered by theoreticians, coming so as a critique to the constructivism way of thinking – socialization. Accordingly, given the fact that representatives of Members States have been cooperating in the EU for decades now, why an extensive number of bargaining processes are not based on a shared understanding of the problem. (Saurugger, 2013)

2.4 Salience - as the intensity of interest

It seems that there is a general agreement of the idea that salience is important in politics analysing, however the same cannot be said about the meaning of salience. Warntjen (2012) provides a useful review of the literature, as he identifies several understandings of salience. Thus, Warntjen (2012) finds that according to Mayhew, 1991, Netjes & Binnema, 2007

salience is related to policy or electoral impact; Achen, 2006 establish that salience is synonym with the terms 'importance' or 'intensity'.

Thomson and Stokman (2006) differentiate between two interpretations of salience used in bargaining models[6]:

- Salience as the proportion of an actor's potential capabilities that is willing to mobilize in attempts to influence the decision outcome.
- Salience as the extent to which actors experience utility loss from the occurrence of decision outcomes that differs from the decision outcomes they most favour.

If the first definition establishes a relational and a behavioural component, the second one does not contain any behaviour reference. According to the first point of view, salience implies that an investment of the interest in one issue can imply that fewer resources are to be spent on other issues and at the same time that an actor would become active in the EU negotiation by mobilizing capabilities in EU decision-making. In contrast, the second definition does not contain any reference to behaviour. However, both views are relates given the fact that a strong utility loss should determine actors/Members States to become more active in EU policies, thus in the EU decision–making process.

As mentioned above, salience is an important component of decision analyses. Building on institutional realism, Achen (2006) identifies salience as "intensity", being the weight factor in a decision analysis. Other theoreticians[7], Coleman (1990) then Konig& Proksch (2006), incorporate salience in the analysis of decisions but taking a distinct point. Therefore salience is seen as an indicator for an actor's interest in an issue and subsequently of the power they invest in defending their stand. However, as Thomson (2011) highlights[8], salience regards the level of interest actors – members states, stakeholders, high officials hold in a negotiation.

Following the line of thought that salience is important in decision analysis Leuffen, Malang & Wörle (2014) have based their analysis of salience formation in EU decision-making on liberal intergovernmentalism line of thought. With the claim that "*societal demands are at the basis of Member State saliences*" (Leuffen, Malang & Wörle, 2014: 629), taking into

[6] Outlined in Leuffen, Malang & Worle, 2014
[7] Outlined in Leuffen, Malang & Worle, 2014
[8] Idem 6

consideration that such demands are to be processed by administrative institutions and governments, the authors introduce also into the analysis factors related to power issues, part of the realism point of view. Testing these suppositions using data from interviews that covered positions of Member States on several issues, the authors have in the end been able to draw a conclusion regarding the formation of salience in EU Member states. According to Leuffen, Malang & Wörle (2014: 629) "*the existence of strong societal demands and administrative capacity – jointly explain overall high level of salience in EU decision making*", however, they find no evidence for "*the phenomenon that a state tries to boost its negotiation success by artificially augmenting its salience on issues*". Thus, in other words, they put forward the idea that salience formation in decision making has a strong connection with national preferences, interests and capacity and no connection whatsoever with power.

According to this findings, the liberal understanding of salience is strengthen, interest group presence strongly impact national saliences. However, it seems that the formulation of salience in EU decision-making process is impacted by the administrative experience of the Members State in the EU (Leuffen, Malang & Wörle, 2014).

2.5. Policy-Making Modes

As the study will mainly deal with decision making process in the EU context, the analysis of Wallace[9] regarding the policy process can be helpful for the research. Wallace defines five different form of EU policy process: distinctive Community method, the EU regulatory model, the EU distributional mode, policy coordination and benchmarking, and intensive transgovernmentalism.

Irrelevant for the topic of this thesis and therefore excluded from the below presentation it is considered to be the EU distributional mode as it envisage financial incentives and EU funding in implementing the provision of the policy/decision. The other four will be shortly presented in order to illustrate the modes of decision making and later on to investigate which method or methods can be applied in the case of the cyber security strategy.

[9] Wallace, H., Wallace, W. (2000) Policy-Making in the European Union, Oxford: Oxford University Press, p 28-35

2.5.1 Distinctive Community method

The notion of Community method illustrates a decision making procedure that ascribe particular role to the European institutions and a particular kind of interaction between them. This theme is to be found in neofunctionalist work and it was argued to constitute a form of supranational policy making, where loyalties were transferred from national to the EU level (Wallace & Wallace in Jorgensen, Pollack & Rosamond, 2006).

Typically, the Community method[10] applies to issues under the first pillar and the procedures of Art. 251 TEC, however over time the method itself has changed as the role of the EP has been extended and an extensive number of policy areas has been included under QMV.

However, it is generally accepted that the differentiation between the Community method and other decision making procedure, as per say the intergovernmental method refers to the influence of the EU's institutions and the Member states on policy outcomes. Even if, in the Community method, the Council (Member States) has considerable influence, given the QMV, it can be the case that a Member State is obliged to implement a decision it is totally against to. (Wallace, 2006)

The main elements of the Community method can be summarised as follows:

•The EC has a strong role in policy making, being the legislative procedure initiator, monitoring policy implementation, with a major role in taking Member States to court if they fail to implement decisions;
•the Council of Ministers decides by qualified majority voting; votes can be obtained through strategic bargaining and package deals;
•as a means of co-decision procedure, the EP is a full partner in the legislative process, role obtain through the time;
•both, EU institutions and the Member States can take cases to the European court

Figure 2 the Community method

[10] Wallace, H., Wallace, W. in Jorgensen, Pollack & Rosamond (2006) Handbook of European Union Politics, Sage Publications, pp 341-344

2.5.2 The EU Regulatory Mode

The EU regulatory model[11] of policy-making has its roots in the international economy. Over time, was employed in developing common market regulation and promoting technical cooperation.

This regulatory mode has been characterized by:

•The EC is the creator and defender of regulatory objectives and rules, working within the policy making with stakeholders and group of experts;
•The Council is seen as a forum for agreeing minimum standards and the direction of harmonization; however, in accordance with national standards and controlled, operated and implemented differentially by the Member States;
•The EP promotes within the rules the consideration of non-economic factors, as environmental and social aspects, but has little leverage on the implementation
•The European Court of Justice watches over the implementation of the rules and allows for cases of non-application or discrimination from states, institutions or stakeholders;
•Stakeholders have, within this procedure, extensive opportunities to be consulted and to influence the content of the European rules.

Figure 3 the Regulatory method

According to Wallace (2006) the EU regulatory mode has been applied to the development of the single market, especially in the area of free movement of goods and capital and less in regards with free movement of services and labour within the EU market.

Furthermore, an outcome of this regulatory mode is represented by the existence of new quasi-independent regulatory agencies at EU level that are responsible within a policy area, as well as partnerships of national agencies working with the European Commission.

[11] Wallace, H., Wallace, W. in Jorgensen, Pollack & Rosamond (2006) Handbook of European Union Politics, Sage Publications, pp 341-344

2.5.3 Intensive Transgovernmentalism

Intensive transgovernmentalism[12] particularly well explains the policy-making process within the security issues. Wallace uses 'transgovernmentalism' instead of well-known phrase 'intergovernmentalism' to emphasize the intensity and commitment in EU level cooperation. This mode of policy implies the cooperation mainly between relevant national policy makers and does not involve intensive participation of EU institutions. This is typical policy framework especially in areas which touch core aspects of state sovereignty. In this case some selected supranational structures can be used, nevertheless member states still keep the privilege of determining types of common instruments and their domestic implementation.

The main characteristics of this policy mode are:

•European Council mainly sets the general direction of policy;
•The Council of ministers controls the consolidating of cooperation;
•The European Commission has limited role;
•The EP and the ECJ is almost excluded from the involvement;
•Special mechanisms for cooperation management;
•The policy process is not open to national parliaments and public.

Figure 4 the Intensive Transgovernmentalism

Critics point to the impression as somewhat loose and weak mode of policy-making. However, it should be mentioned that this method has the capacity to bring out substantive and effective joint policy when needed.

Moreover, one should remember that this policy mode develops in areas where EU level of integration is now emerging or which has been long under the national control. Therefore, it might be misleading to compare the integration in such areas with the integration in less sensitive policy areas such as environment or commerce. This kind of cooperation employs

[12] Wallace, H., Wallace, W. (2000) Policy-Making in the European Union, Oxford: Oxford University Press, p 34

'soft' institutions, which have little autonomy, and binding power, nevertheless have quite good potentials of generating 'hard' policies.

2.5.4 Policy Coordination and Benchmarking

Another relevant EU policy-making mode is policy coordination and benchmarking[13], which stems from the experience of the Organisation for Economic Co-operation and Development (OECD); it developed practice of comparing and evaluating the public policies of each state.

Therefore, sometimes it is called 'OECD technique'. The EC usually uses this technique to build up light cooperation in a new area in order to bring this issue eventually to the supranational level, as it did in case of environmental policy issue by achieving the incorporation of this issue to the Single European Act (SEA). This policy coordination therefore, counts mainly on technical specialist opinions and assumptions to develop a common approach, to encourage innovation.

The main features can be defined as:

•The Commission is a developer of a network of experts;
•'Independent' experts are engaged as promoters of ideas and techniques;
•The high-level groups in the council are organized for brainstorming rather than negotiating, thus the Council also has creative character;
•Dialogue with specialist committees of EP in specific issues.

Figure 5 the Policy Coordination and Benchmarking

It is observed that, this coordination practice is not any more merely a technique for transition, but became a policy mode itself. The opportunities of using 'benchmarking' together with coordination at EU level produced advanced chances for comparing national, local and sectorial practices.

[13] Wallace, H., Wallace, W. (2000) Policy-Making in the European Union, Oxford: Oxford University Press, p 33

Moreover, this is being done not for the sake of generating a single policy framework, but for sharing experiences and support the spread of best practice. With its practicality and emphasis on actual work, this policy mode is seen as a persuasive alternative to the before existing formal ones.

One main feature of this mode is that it is based on intergovernmental ground. However, if we look the purpose of using this policy, we can see the supranational character also. Benchmarking at EU level aims towards improvement and changes in performance in certain issues and for supporting certain policy. It should develop key indicators for comparing and evaluating, and help to understand why and how the best practice has been achieved. Benchmarking itself can be viewed, on one hand, the promoter of Europeanization by leading to convergence of national policies; on the other hand, the 'nationalization' of policy areas, by introducing only the best national practice.

2.6. Theory discussion

As seen above, several theories and perspectives regarding decision making within the EU were brought forward. Every theory illustrated offers different perspectives in regards with the decision making process within the EU. In this section, I will discuss the theories, explaining their added advantage for the subject at hand. Within the end of the subchapter, I will put forward hypothesis that arise from the theoretical framework that could explain the problem under investigation.

Liberal intergovernmentalism, new institutionalism and the constructivist thought are to be used within the thesis to help me identify which theoretical perspective can explain the process of adoption of a cyber security Directive in the EU.

The policy mode approach will be used to assess which path was followed in the cyber security issue and offers insights into what is to expect in the area.

Within the liberal intergovernmentalism theory it is argued that national preferences are shaped by the economic interest of powerful groups, most common at national level. Agreements reflect the finality of national preferences and bargaining power of the Member State. International institutions are established given the characteristics of the issues they are

supposed to manage; therefore their power is restricted to that (Moravcsik & Schimmelfennig, 2009). Thus, MSs preferences and policy views are not affected by the participation in this institutions.

On the other hand, new institutionalism argues that decisions are made within institutions and that the EU institutions are not merely at the Member States discretion and preference, but they form such preferences. Therefore, the participation within EU's institutions and the solely EU membership are factors that shape preferences and influence decision-making.

The constructivist thought follows the institutionalism idea of the importance of institutions, however it is added the fact that they are forums for changing behaviour. Introducing the socialization terms, theoreticians put forward a line of changing norms and preferences based on cooperation within groups in regard with policy making. Thus, decisions are not merely at the states discretion, they happen within groups that in time change their preferences, interest and position in respect with the group's position. In this regards, one can put forward the idea that national representatives working in such groups , in time, will not represent the MS's interest and position, but they will come closer in line of thought and achieve common policies according to the general EU's interest and views.

***

Looking at the theories illustrated within this chapter, one can easily conclude that there can be different ways of decision making at EU level and in each situation specific elements characterize the process. Therefore, from the theories, the following variables can be outlined:

(i) costs and benefits of interdependence,
(ii) role of domestic groups,
(iii) normative institutionalism (role of institutions),
(iv) salience

The outlined variables are to be used with the empirical part of the thesis in order to follow up on the negotiation process for the NIS Directive. Moreover, the first three variables will be employed in identifying hypothesis in connection with the decision making process within the cyber security field in EU. Additionally, the salience variable will be employed to illustrate the MSs intensity of interest attached to the issue.

Thus, drawing from the theories, the following hypothesis can be put forward:

1. **The decision making process within the cyber security field is predominantly of intergovernmentalism influence**

Such hypothesis can be proven by looking at the negotiations for adopting the NIS Directive. The following elements are able to prove an intergovernmental approach in decision making:

- if there is strong evidence of a cost and benefit interdependence;
- if there is pressure of domestic groups and changes illustrate that their concerns were dealt with;
- if the Council, thus the member states, pose much influence within the negotiation and has managed to push forward its own agenda.

2. **The EU institutions are key players within the decision making process**

The EU's normative and policy commitments impact the participants to the decision making process. Of great importance within the negotiation process is the role of the EC, the EP and the working groups within the Council. Changes that occur in the negotiation phase are merely to support the general interest of the Union, as MSs preferences are shaped within the process and thus cooperation characterize the process. The constructivist approach comes here to fortify the influence of EU institutions within the decision making process, as socialization that occurs within the EU institutions helps also in forming the actors interests.

III. Methodology

Methodology refers to the background, theoretical, political and philosophical assumptions, of social research and their implications for the research and for the use of particular research methods. (Kuada, 2014) Thus, methodology is transcribed in what I will call next the Research philosophy. Additionally, this chapter is meant to describe the path I will follow in carrying out the research, thus the methods. Moreover, this part of the thesis will account for a motivation of the chosen methods, sources, as well as the empirical material used.

The idea of investigating the process of decision making when talking about a common cyber security policy caught my attention while researching for the EU's position on cyber security and cybercrime.

Basically, given that this is an area of great importance, due to the fact that nowadays the Internet and ICT cover all aspects of our life and the EU has long ago stressed the importance of international collaboration to increase protection, until now within the EU there have not been any common accepted standards. Thus I believe that is interesting to analyse the process of decision making and policy harmonization within an area in continuous development in the context of connecting theoretical approaches and reality.

3.1. Research philosophy

Ontology represents the way we see the reality and how we understand existence. On the other hand, epistemology talks about knowledge and the way in which one can obtain it.

Within ontology one can take the Positivism approach, the reality being independent in regards with the observer, thus the researcher will have an objective epistemological stand point. In the opposition situates the Interpretivism, where knowledge is relative to the observer, thus taking a subjective epistemological position. (Prinsted, 2013)

As I will sustain in the following part, within this paper qualitative methods are used in order to tackle the problem. Thus, I will take an interpretivist approach within the analysis, as the qualitative methods are premised upon a belief that the observer cannot detach him/herself completely from the object of research. (Kuada, 2012; Prinsted, 2013, Kuada 2014)

3.2. The Qualitative method - Documentary analysis

The documentary analysis within the qualitative method of research refers to the review of written documents that can take many forms, for example textbooks, articles, notes, minutes of meetings, archives etc.

Documents used within the research may have already been part of the public domain, as is the case of the paper at hand – reports for the EU's institutions for example - or are created as part of the research study. As stated by Robson (2011), it is important within this method to identify the context of the used document, by establishing the author and the purpose.

3.3. Case study and analysis

The present paper traces the evolution of the EU's Commission Directive for Cybersecurity from proposal towards its adoption. It is based on an investigation of the continuous negotiations between the European Parliament, the Council and the Commission as to reach an agreement for a common cyber security policy.

The study case will therefore check out the aspects that have changed within the directive text, taking into consideration the variables that may affect the decision making in the EU.

The outlined analysis will connect those changes with the existing theory; the paper will shed light on the nature of holdbacks within the process of approval of the NIS Directive.in order to push forward a framework in regards to the decision making in the EU in relation with cyber security. This will be done more simply by checking which hypothesis that emerged from theory applies to the present case study.

The novelty of this paper is offered by the analysis of the factors that explain how one can understand the changes within the Directive. Additionally, I consider that such analysis could have a practical applicability for the development of a coherent approach in adopting a common policy in the area of cyber security. Identifying different positions is vital in working to overcome the respective issues and move forward to a common ground.

3.4. Empirical data and sources

This section contains a presentation of the data and sources that are used in the paper. The relevant data and sources will be presented and explained - from where it was taken, how it has been collected and what considerations to have regarding its credibility and objectivity.

In order to lead the analysis down to the answer for the problem formulated prior, I have chosen to extract data from legislation, statistics and international publications that regarded the aspects involved in this project. As an important part of the analysis, I consider more opportune to first detail the data in the Case Study – the empirical data chapter. This will happen, on one hand, to show the empirical data from the start, so the reader could have an overview of the analysis that follows. On the other hand, because when the analysis asks, it will be easier to refer to the explanatory section.

In this project all the data collected is secondary. The secondary data is represented by the data collected from other sources, and not developed by the researcher himself; unlike primary data which is gathered by the researcher before or during a project. I have chosen to use secondary data as the subject of concern is very present in the contemporary world and the data gathered by institutions and organizations with adequate resources are more valuable.

Quantitative and qualitative research and data

Quantitative research was not undertaken as part of the paper as it was considered out of the scope of the research. Given the fact that I want to illustrate the changes in the Cyber security Directive and how such changes reflect on the theories of International relations, and what can be applicative within the EU decision making process, a qualitative research is more appropriate. Thus access to qualitative data, such as legislation, official reports and papers, was sought. This data is reliable, as the sources are the European Union outlets and Member Countries official position. Therefore official websites from EU and MSs were accessed and official publications were researched online.

Ontologically, qualitative research is seen as being subjective. It has the purpose to provide a deeper understanding in a given matter, with the aim of interpretation of the subject. (Zang&Nielsen, 2013) Giving the fact that in this case knowledge has been in some cases interpreted by scientists, it has to be consider that the external reliability is diminished, due to

the possibility of being interpreted different from one theoretician to another. In this project, Media articles picturing event within the project context and scientific analysis of actors represent part of the qualitative data. Even though the data is subjective, the information revealed by these sources will play an important part in the discussion section of the analysis, because they can clearly show certain positions.

Here, the empirical data has a central role, given the choice to use legislation in relation to theory to make the foundation of the project and the data within the impact assessment's explanatory part to show the development of the decision making process and possible outcomes.

The legislation data of the project is composed by European strategy in regards with cyber security and the proposed directive and by MSs legislation and external policy. The source from which the European data is gathered is the European Commission and EU Council reports and other official papers.

The legislation has been chosen as a source of qualitative data for this project due to the fact that transposes the EU's intentions into practice, giving valuable hints of the EU's position.

The Media articles are used in order to follow and present the events in a developing problem as promptly as needed. The Media sources that were followed are newspapers. There were no political or ideological aspects taken into consideration in the choice of the specific source, the criteria used to choose the newspapers which the articles are taken from, is the importance of the newspapers, internationally and also at national level and the coverage of the subject. The most important selected sources were:

- Reuters (reuters.com): international news agency with international coverage and with a strong policy towards upholding journalistic objectivity.
- EurActiv Media Network (euraktiv.com) a leading EU affairs online media, present in 12 EU capitals, publishes free EU news and facilitates EU policy debates for policy professionals[14]; 667,494 average monthly unique visitors across EurActiv websites.

[14] http://www.euractiv.com/concept

Empirical data limitations

Empirical limitations come to show an empirical framework within which I intended to develop the project's analytical part. The inclusion of interviews and statistics are options already restrained due to limits of time and size of the project. Furthermore, interviews and declaration of officials were followed and some are to be presented in the empirical part. However, I have chosen to not proceed in realizing interviews as the possibility of inconclusive responses was considered, among others like reliability (to reach a person of decision in the process is hard and it may be the case that an official position cannot be expressed yet), resources, etc.

Statistics and financial data put forward by member states and the EU's institutions were consulted in order to provide a clear image of the current situation and the outcomes of the Directive.

3.5. Choice of theory

This part will come as a justification of the choice of theories and will present my motivations in using the previous detailed theoretical framework.

Given the fact that the problem for analysis is complex, it is understandable that a single theory cannot explain it in depth. Therefore, the theoretical framework is based on three main theories, namely liberalism, institutionalism and constructivism. As shown within the theory analysis, these theories will be used in explaining and analysing the problem under discussion. They are used in creating hypotheses in connection with the decision making process at EU level in connection with the cyber security directive and in the end will be used to illustrate the applicable path in EU policy harmonization in the cyber security sector.

Furthermore, although the first hypothesis can be explained to a certain extent also through the security theory, I motivate my choice of analysing it by using primarily the liberal intergovernmentalism approach of Moravcsik through its greater relevance for the hypothesis. Also, while taking into consideration the national preferences and interest, Moravcsik employs the role of pressure group in consolidating the national interest.

Within the second hypothesis I have chosen to use both the institutionalism and the constructivism approach as I believe that they complement each other in pushing forward a stronger conclusion. Both the norms and the socialization aspect of the EU's institutions contribute to the increased role of shaping interest attributed to the institutions.

The theories chosen are used as a tool to assist the investigation of the on-going process of negotiation for the NIS Directive and will come to support the identification of the type of the decision making process within the cyber security field; thus the approach of this thesis will be deductive, equally descriptive and explanatory.

Limitations

These theories have been chosen in the detriment of the security theory for valid reasons. First of all the aim of this paper is to investigate on the decision making process within a new field of power for the Union, on the policy harmonization and the changes that arise within the negotiation for new legislative framework within the EU.

In this paper, I will not try to challenge the theories, but I will use them in searching for an answer to the problem formulated. The theories will help illustrate the pattern used in the decision making process in the cyber security process and will further illustrate how the reality is constructed. Therefore, as previously shown each theory helps develop a hypothesis that will support the investigation and the analysis in order to find an answer to the formulated question.

IV. Empirical data

This chapter is meant to create an overview of the reality of the EU's proposed Cyber Security Directive and to provide punctual data on the process of approval.

In this regard, the Directive's content and the changes within the text are to be illustrated in relation with the affected parts.

The data presented within this chapter, together with the theories will constitute the foundation of the analysis incorporated in the fifth chapter of the thesis.

4.1. EU's Cyber Security Directive

As mentioned in the Introduction, as part of the European Union's Cyber Security Strategy, published on 7 February 2013, the European Commission proposes a Network and Information Security Directive (NIS Directive), commonly known as the Cyber Security Directive.

Cyber security is one of the biggest issues that governments and businesses in the EU and globally are currently facing. According to the Commission's consultation, 57% of respondents had experienced information security incidents over 2011 (Commission, 2013a), while the UK government has rated cyber security as a Tier 1 threat to national security (UK Cyber Security Strategy, 2011).

4.1.1. Directive's approval process

Following the Commission proposal from February 2013, the Directive has been subject to several negotiations between the Commission, the European Parliament and the Council of the EU. The proposed Directive is being negotiated and adopted through the ordinary legislative procedure;, the Council co-legislates with the European Parliament.

The text-box below outlines the ordinary legislative procedure.

The main legislative procedure by which directives and regulations are adopted, formerly known as the co-decision procedure, it is illustrated in the below figure.

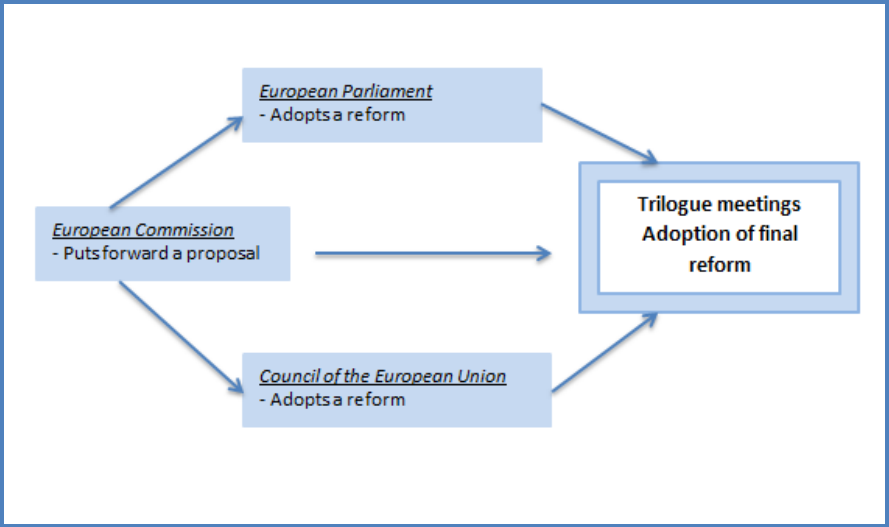

Figure 6 Ordinary Legislative procedure

The commission submits a legislative proposal both to the Parliament and to the Council of the European Union. At the first reading, the Parliament adopts its position. If the Council approves the Parliament amendments, the act is adopted. In opposition, the Council will adopt its own position and forward it to the Parliament. At the same time, the Commission has to inform the Parliament regarding its position. Within the second reading, if the Parliament approves the Council's amendments the law is adopted. If the Parliament rejects the Council text the law fails or it may be decided to modify it and therefore the proposal will return to the Council.

If the new text is not approved by the Council, a Conciliation Committee formed by members of the Council and MEPs and monitored by the Commission, will be convened. A positive agreement on a common text and approval from both the EP and the Council will transpose in successfully adoption of the law. In case of disagreement within the third reading, the act fails.

Figure 7 the Ordinary legislative procedure

Within the Council, following preparatory work by the Working Group on Telecommunications and the Information Society (WP TELE), an initial orientation debate on the draft directive was held on 6 June 2013. (Council, 2015)

Moreover, within its meeting for 25 June 2013, The General Affairs Council (the European affairs ministers from all EU member states) welcomed the European Commission published Strategy and the proposed Directive.

Within the Transport Telecommunications and Energy (TTE) Council meeting on 5 December 2013, ministers took note of a progress report on the directive dated 22 November 2013. The report highlighted on-going preparatory work on issues such as:

- the scope of the directive,
- the terminology used,
- the set-up of the cooperation network, and
- the requirements for the national NIS strategies.

Following its course in the European Parliament, in March 2014 a modified text of the proposal for a Network Information Security Directive was adopted. The amendments were drawn up by the internal market committee (IMCO), as leading committee in association with the industry (ITRE) and civil liberties (LIBE) committees. (European Parliament, 2014)

A new progress report, dated 22 May 2014 was further discussed in the Council within the TTE meeting on 6 June 2014. According to the Council[15], the ministers tried to identify best ways to cooperate in order to improve the preparedness and reactions to cyber security threats. Additionally, they emphasized on the operational cooperation that takes place within different bodies and agreed that discussions on the practical arrangements for cooperation should continue. Moreover, all delegation agreed that "*the priority in the Directive should be on strategic/policy cooperation*" (Council, 2014:10).

At the TTE Council meeting on 27 November 2014, under the Italian presidency, the state of work on the draft NIS directive was presented. It was pushed forward that the main issue between the Council and the Parliament position is the scope of the proposal, namely the operators that are to fall under the Directive's requirements and who is to decide this.

[15] http://www.consilium.europa.eu/en/policies/cyber-security/

As stated in the Council paper[16], the Council version allows Member States to assess based on specific criteria, certain operators in the specified fields that should be subject to the obligations set forward in the Directive in regards to security requirements and incident notification.

On the other hand, the already voted European Parliament text, makes subject to the obligations regarding security requirements and incident notifications all operators within all sectors, the only variable consisting in the degree of providing evidence for the effective implementation of the security policies.

Thus, the object of difference between the two parts, the MSs, represented by the Council and the EU's institutions (the Commission and the Parliament) is the body of decision – who should decide what operators fall under the scope of the Directive. In other words, the member states want to have the power and liberty to decide which operators fall under the scope of the directive. On opposition, the EU is inclined towards a supranational exhaustive list of operators and sectors.

Given the distinct positions, at the end of 2014, assisted by the Commission, the Council held two trilogue meetings on the directive with the European Parliament and the EU Commission. The Member States position differs, in several areas, from the one pushed forward by the Commission and also by the Parliament adopted version. In order to exemplify such difference of opinion the below picture can be used as reference. Several examples of the differences in opinions are to be found also in **Annex 1** – *Positions of co-legislators*.

[16] Council of the European Union (2014) Information on the state of play

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
concerning measures to ensure a high common level of network and information security across the Union
COM (2013) 48 – 2013/0027 (COD)

COMMISSION PROPOSAL *COM (2013) 0027*	**EP AMENDMENTS** *P7_TA- PROV(2014)244, 13.3.2014*	**COUNCIL AMENDMENTS** *10153/14* ***(As submitted to Coreper 07.11.2014)***	**POSSIBLE COMPROMISE SOLUTIONS/EP PROPOSALS/COMMENTS**
2. To that end, this Directive:		2. To that end, this Directive:	
(a) lays down obligations for all Member States concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems;		(a) lays down obligations for all Member States concerning the prevention, the handling of and the response to **serious** risks and incidents affecting networks and information systems;	The term "serious" is under discussion with the EP
(b) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems;	(b) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated, ~~and~~ efficient ***and effective*** handling of and response to risks and incidents affecting network and information systems ***with the participation of relevant stakeholders***; (AM 40)	(b) creates a cooperation **group** ~~mechanism~~ between Member States in order to **support and facilitate strategic cooperation and the exchange of information among Member States** ~~ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response~~ to risks and incidents affecting ~~network and information systems~~;	Provision to be aligned with art. 8a(1) after the agreement on the latter article
		ba) creates a CSIRTs ("Computer Security Incident Response Team") network in	Provision to be aligned with art. 8b(1) after the agreement on the latter article

Figure 8 Positions of the co-legislators following the 2nd informal Trilogue;
Source: Council of the European Union (2015) State of play and work ahead

As illustrated above, EP amendments to the text pushed forward by the Commission have preceded the approval in the European Parliament of the NIS Directive. However, the Council, to be understood as the Member States, has different opinion and following the informal meetings held in 2014, a common ground has not been reached yet.

A third trilogue meeting took place on 30 April 2015. Although, according to the Council, progress was made during the past meetings, still important differences remain between the Council and European Parliament positions. Therefore, another trilogue meeting is expected, although the date has not been published.

Given the state of these discussions, I will further present in this part, the changes that the Council proposes to the NIS Directive's text and the EP's position on such agreement. Moreover, the difference between the version proposed by the Commission and the possible outcome, as wished by the Member States will be presented. Such illustrations will be made in relation with the impact that will fall, either on MS or on market operators if such changes are to be made.

4.1.2. Directive's content

The five main elements of the proposed NIS Directive are listed below:

- **Establishment of a National Strategy and Competent Authorities**

Within the Directive (Chapter II), it is required for Member States to ensure the security of the network in their territories. Thus, it is required for MS to adopt a national strategy that sets out concrete policy and regulatory measures to maintain a level of network and information security. This includes for them to appoint a National Competent Authority (NCA) for information security that monitors and ensures consistent application of the Directive and setting up a Computer Emergency Response Team (CERT) that is responsible for handling incidents and risks (Commission, 2013b). The version approved by the EP allows Member States to designate several National Contact Authorities (NCA) as long as only one national authority remains responsible and accountable, and permits for more than one national CERT (European Parliament, 2014).

Therefore, the Member States will have a single authority accountable for monitoring the compliance with the Directive, promote the Network Information Strategy and receive, gather and share information regarding cyber security threats. Moreover, the institutions will support Member States to develop the minimum security requirements and encourage businesses to create ICT security plans.

There are Member States that already have in place a National Cyber Security Strategy and national CERTs, but also member states that have not implemented such legislation and created bodies to be responsible for cyber security within their borders. Some examples in this regards are to be find in **Annex 2 – Cyber Security within European Union - Country Summaries**. The information presented there is a descriptive illustration of the national state of play in regards to cyber security in several MSs.

Co-operation network

The competent authorities in EU member states and the European Commission will form a co-operation network to co-ordinate against risks and incidents affecting network and information systems. In the latest version of the text, after the approval of the EP in 2014, ENISA is also included in the cooperation network[17].

The cooperation network will:

- exchange information between authorities and the Commission,
- provide early warnings on information security issues,
- agree on a co-ordinated response in accordance with an EU NIS co-operation plan.
- Cooperate with relevant European bodies, as European Cybercrime Centre

Following the amendments from the EP, the cooperation network established between NSAs, the Commission and ENISA will also have the following roles[18]:

- involve, consult and exchange information with market operators in regards with risks and/or incidents affecting their network and information systems
- develop guidelines for notification of incidents (in the term of sector specific criteria)
- publish a report each year to include activities of the network in concordance with provisions laid out the preceding year.

Moreover, this cooperation network will be created with the scope of permanent dialog and support, as Member States are to inform within the network of risk and incidents that may exceed national response capacity or that may affect more than one state.

The directive does not provide guidance for situations when MS cannot agree on a coordinated response to a cyber-threat as the process of seeking agreement might slow down the response and, at the same time, coordination across different MS might be challenging to achieve, as security levels differ. However, the Union NIS cooperation plan that is previsioned to be adopted within a year of the Directive's approval will include such guidance.

[17] Amendment 76, Proposal for a directive; article 8-paragraph 1
[18] Amendment 78, Proposal for directive; article 8-paragraph 3

Security requirements

A key element of the proposal is that Member States must ensure that public bodies and certain market operators take appropriate technical and organisational measures to manage the security risks to networks and information systems. Thus, a level of security appropriate to the risk must be guaranteed within public bodies and market operators and, moreover, they should prevent and minimise the impact of security incidents affecting the core services provided.

Additionally, they are under the obligation to notify the competent authority of incidents that have a significant impact on the continuity of these services. Following such notification, the competent authority will decide if necessary to inform the public of the incident or not. In such regard, according to amendments by the European Parliament, the significance of the incident should take into account when informing the wide public:

- The number of users affected;
- The duration of the incident;
- The geographic spread of the area affected by the incident.
- There has been a lot of discussion over who should be included as a market operator.

As the first draft set forward by the Commission defined:

- market operators to include information service providers such as internet payment gateways, social networks, search engines, cloud computing providers and app stores,
- operators of critical infrastructure, such as electricity and gas suppliers, operators of oil and natural gas, air carriers, maritime carriers, railways, airports and ports, traffic management operators, banks, financial market infrastructure and health care providers.

Following the European Parliament amendments of the text, it was decided that the requirement to report the above-mentioned incidents should be limited only to critical infrastructure operators and market operators should voluntarily report such incidents. The EP has concluded that the inclusion of information services providers in the scope of the Cyber security Directive was "disproportionate and unmanageable"[19]; however organisations

[19] European Parliament – Legislative Observatory, http://www.europarl.europa.eu/oeil/popups/summary.do?id=1342725&t=e&l=en, accessed on 13.04.2014

that provide network operators with Internet traffic exchange facilities were added to the list of critical infrastructure operators.

It is believed that the exclusion of Internet enablers from the extent of the Directive could reduce its effects, given the importance of these operators within the online medium and the economy (Ryan, Buckenham and Donnelly, 2014). Moreover, as more of critical infrastructure operators' functions become digitised they are bound to engage in cooperation with software developers, cloud storage providers, e-commerce platform, etc. and therefore, it is becoming difficult to set a clear distinction between these categories.

Another amendment brought by the Parliament offers Member States the choice to include public administrations under these security requirements, given the fact that the original text obliged them to do so. Such elements are viewed as threats to the effectiveness of the Directive[20], as the Cyber Security Strategy clearly points out towards the relevance of all stakeholders, being public authorities of private sector, in taking actions to strengthen cyber security. (Commission, 2013c)

- **Use of standards**

In order to ensure convergence of policy implementation, Member States are encouraged to use NIS standards for the implementation of the security requirements on market operators. If in the Commission's proposal the institution was responsible to draft such standards, the revised text approved by the Parliament sets out the European Commission obligation "to give mandate to a relevant European standardization body" (European Parliament, 2014 - amendment 122, Article 16, paragraph 2), which will establish a list of standards and/or specifications, following consultation with relevant stakeholders.

- **Enforcement**

The competent authorities and NCA in each Member State are to be given powers to ensure compliance of market operators with the Directive, which may include asking for evidence of effective implementation. Thus market operators may be required to undergo a security audit; same provision may be applied also to public administrations, if the Member State considers so.

[20] Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda in the Plenary debate on Network and Information Security Directive, Strasbourg, 2014

The competent authorities may also report criminal incidents to law enforcement authorities. Additionally, when incidents involve personal data, the NCA should work in cooperation with data protection agencies. The revised text approved by the Parliament set forward the obligation of NCA to develop together with data protection agencies and ENISA information exchange mechanisms and a single template to be used under both the Cyber Security Directive and other EU law on data protection. (European Parliament, 2014)

4.2. Impact assessment of the NIS Directive

The proposal for a NIS directive would incur costs to Member States, covered entities (both public and private organizations) and, of course, the Union. These costs will mostly come from these following main provisions[21]:

- Establishing of a CA at national level;
- One or several national CERT's;
- Administrative burden, both for public and private organizations through setting up security programs and hiring of additional staff;
- Secured network in order to allow the sharing of incident reports and other relevant information to the CA;
- Investigating breaches, where significant breaches will of course last longer and for a higher cost.

a. Establishing of a CA at national level

The costs incurred by the NIS directive vary greatly amongst the Member States, mainly because of the discrepancies between the existing infrastructure and its level of preparedness in each state. In regards to the designation of a NIS central authority, it is more likely that the Member States will designate one of the existing bodies, instead of establishing a new one. The existing bodies will most likely have additional tasks for which they will probably need

[21] In providing this overview of impact of the proposed NIS Directive information were retrieved from several EU and national documents, among the most used were EU's Commission Impact assessment accompanying the NIS Directive (2013a) – referred further as Commission's Impact assessment (2013), European Parliament Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts (2013) – referred further as EP (2013)

increased workforce, which will be regarded as additional Full Time Equivalents (FTE's). The Member States that already have enough staff in place will most likely incur no extra cost.

b. One or several CERT's

Currently there are three Member States that do not have an existing national/governmental CERT (Cyprus, Poland and Ireland, although the latter is currently in the process of developing a national cyber-security center). The estimated cost of setting up and making it fully operational is thought of as being 2.5 million EUR per CERT. This estimated cost has been provided through a series of discussions carried out with already established and operational CERT's. (Commission, 2013a)

c. Administrative burden

The administrative burden is to be experienced both by the public and private organizations through setting up security programs and hiring of additional staff.

Based on discussions and consultations with several national designated NIS bodies, the European Union advanced that a number of 6 FTE's will be required for the functioning of a national CA. The FTE's would be in charge of developing and implementing a cyber-strategy cooperation plan and the national cyber security strategy. The cost advanced by the European Union is of 360.000 EUR for each member state, thus a total of 9.72 million EUR for the entire Union. The total cost would be much lower since several Member States already have cyber security centers and bodies in place. Given the diversity of existing cyber-security organizations in the member states, this would be a very broad estimate.

Looking at the EU' Cyber Security Maturity Dashboard 2015 (Annex 3) a research undertaken by BSA, the Software Alliance shows that less than 20 of the 28 Member States have more or less detailed and comprehensive cyber security strategies in place, while eight have not declared such framework at all. Moreover, even the countries that have already adopted such strategies encounter differences between the quality of the framework and a clear implementation plan is missing.

Furthermore, most of these documents seem static. Only a small number of countries have already revised and improved their initial strategies and published an updated one. Finally,

only a minority of the Member States have reinforced their cyber security strategy with relevant legislative and policy instruments that address security, information classification obligations and critical information infrastructure protection requirements. Therefore, there is a need for almost all EU MSs to invest in developing its national framework. Thus, the burden will fall also on those that have already established strategies, in order to reach the standard established by the EU's NIS Directive.

In regards with the private sector, the compliance costs for NIS implementing have been calculated as the difference between the target level of spending according to current best practices and the current level of spending in the various relevant sectors. The target level is thought of as being around 6.61% of a company's budget, which is lower than the average given by the Information Security Breaches Survey by PWC, 2013, which shows that SME's spend around 12% of their budget on IT security. An exact cost is difficult to approximate, given the differences between SME's in regards to their current capabilities and level of preparedness and security. Another factor which is difficult to anticipate is the advancement of technology and its future costs. One area which is currently viewed with increased interest is cloud computing. The appearance and development of cloud computing has revolutionized the security strategy of a significant number of SME's. Thus, they can reduce the number of security measures that have to be implemented and overall the costs regarding IT security. A strong development of the cloud computing concept in regards to security and easy access and functioning will undoubtedly have a strong impact in reducing the overall costs of implementing the NIS directive. (European Parliament, 2013)

Although there already are high levels of spending for public administration and key private players in regards to IT security, the European Union believes that in order to comply to the NIS regulations there will still exist an additional cost in the range of 1 -2 billion EUR. It is estimated that around 42,000 market operators and all EU public administrations will be affected. The cost of compliance to the NIS directive is estimated to be between 4,000 EUR and 50,000 EUR per year, depending on business size. The total estimate of 1-2 billion EUR also takes into consideration that most companies and public administrations would already have high security protocols in place, in order to comply with the existing regulations and provisions. The extent to which the NIS directive would overlap with the already established provisions is difficult to estimate, but it is assumed that the overall overlap will be

considerable. Furthermore, it is expected that a significant amount will be spent by the actors that fall within the scope of the NIS directive for compliance with other regulations than the NIS directive. The required spending will be made naturally, out of commercial or good governance reasons. Out of the 1-2 billion EUR estimated for compliance to the NIS directive, the public sector accounts to over half of this amount (between 577 and 1.155 million EUR). (Commission, 2013a; European Parliament, 2013)

d. *Secured network in order to allow the sharing of incident reports and other relevant information to the CA*

The flow of information regarding incident reports and other relevant information between competent authorities and CERTs will be done through a secured network. The costs for this depend on whether an existent infrastructure, such as the Secure Trans European Services for Telematics between Administrations (sTESTA), will be adapted and used or a completely new dedicated infrastructure will be set up. The former bears a cost of around 1.25 million EUR (based on the cost of the adaptation by the European Commission's Joint Research Center) for the public health early warning and response system and can be done using EU's budget. Alternatively, the cost can be shared between member states.

In the latter case, the costs for setting up and implementing a dedicated infrastructure have been estimated at around 10 million EUR per year for all EU (based on incurred costs by the EC in relation with sTESTA) and would have to be shared between member states.

e. Investigating breaches, where significant breaches will of course last longer and for a higher cost.

Regulation costs are often expressed in terms of additional time (hours, days) that is required on a yearly basis. The average yearly gross salary per FTE for the EU 27 is considered to be 60 000 EUR.

As the provisions of the Directive are not yet in place in the Member States, only in the process of being implemented, the overall costs regarding breaches are based on estimates of the data available from the provisions and regulations of the electronic communications sector, through Art.13 a and b of the 2009 Revised Regulatory Framework for Electronic Communications.

Breaches will have to have a possible significant impact and outcome in order for them to fall under the NIS directive scope. The first ENISA annual analysis of Art.13 incident reports estimates the number of incidents at 510 for the electronic communications sector for the year 2012. Given an estimate of 12000 relevant electronic communication companies under the NIS directive, it accounts for 4% of companies in this sector. Maintaining the ratio and applying it to the total of 42 633 companies in the scope of the NIS directive, the number of expected breach notifications will be around 1700 on an annual basis.

Within the European Commission (2013a) Impact Assessment, a duration of 0.5 working days is taken into consideration for each breach notification, with a cost of 125 EUR for each. Therefore, the total cost for notifying breaches on an annual basis will be 212500 EUR at EU level. Thus, it is assessed that given the low volume of breaches estimated to fall within the NIS Directive scope and a relatively reduced investigative cost for each case, the final cost for reporting and first hand investigations would be relatively low for all stakeholders concerned.

In the event that a security breach has to be further investigated, costs are of much higher amplitude. Out of the estimated 1700 security breaches reported on an annual basis, it is estimated that between 10% and 20% will be further analysed, corresponding to 170 to 340 investigations per year. Several aspects have to be taken into consideration in order to determine the actual cost of the investigation. Within those aspects, the methodology decided by the MS and the level of complexity of the investigation are considered the most relevant ones.

Taking into consideration the standard salary defined above, investigating a single breach in a worst case scenario would bear costs of maximum 25 000 EUR, leading to a total of 4.25 million EUR up to 8.5 million EUR per year across the European Union. (Commission, 2013a)

4.3. Technical discussions in formal and informal meetings between EU's institutions

As presented in the first subchapter, since 2013, a series of meetings and discussions have taken place in order to push forward the NIS Directive.

Following the approval of the European Parliament with several amendments, agreed also by the Commission, the Directive needs the approval of the Council in order to enter in force. As seen in the Directive's approval process subchapter, the Member States, as represented by the Council, have different opinions and an agreement has not been reached yet in the negotiations between the Council, the EP and the Commission.

Discussions between the three parts were held with the scope of finding common ground and though a series of bargaining to push forward a mutually agreed solution, as a common view on the issues does not exist.

However, as seen from the official documents, the Committee of Permanent Representatives (COREPER) facilitates such discussions, but ultimately the MS delegations are to compromise for the issues under negotiations. Under this forum, COREPER is empowered to represent the Council, but cannot agree on any solution. (Council, 2015)

Therefore, agreement has to be found between the Commission, the European Parliament and the Member States delegations. In terms of subjects under discussion, according to official document from the Council dated January 2015, compromise is necessary in regards with "*two main political issues under negotiation, i.e. cooperation and scope*". (Council, 2015:2)

As is presented in the above mentioned document, the flexibility of the EP in terms of cooperation provisions has to be shown also by the Council in terms of scope of the Directive.

Within *cooperation*, the Council trusts that the EP can accept its proposal to replace articles that envisage the establishment of a Cooperation Network, as per the original proposal, with two new articles that establish the creation of a *Cooperation Group* and a *CSIRTs Network*. However, according to the Council such compromise can be accepted by the EP in case of a clear structure for the operation of the two bodies translated in clear timeline and effective governance. (Council, 2015) Put in other words, the EP wants to have the certainty of

cooperation between the MSs, with some clear check-points within the Directive text that will enable such cooperation. Thus the terms and structure of the cooperation mush be made known beforehand. Including such elements in the Directive's text will clearly illustrate the relations between MSs and EU's institutions and Mss will be obliged to follow the prior established structure.

Thus, according to the Council, a compromise text was formulated, entailing progress on cooperation and assessment of such progress, clear timeline and a cooperation system driven by the MSs and supported by ENISA. Moreover, it is to believe that such compromise text will be put forward in a final version of the Directive's text, as the Council states to have the same interest in the issue as the EP. (Council, 2015)

A different negotiation procedure can be observed in the case of several parts that the EP agreed to remove from the Directive's text in order to obtain the Council "flexibility with regard to the issue of scope" (Council, 2015:2). The areas under negotiation here were *article 9* establishing a "**Secure Information-Sharing System**", *article 10* "**Early Warning**" (however included in *article 14* of the same directive), *article 11* "**Coordinated Response**" and *article 12* adoption of a "**Union NIS Cooperation Plan**" by the Commission.

In terms of the issue of *scope,* a compromise between the Council and the EP has not been reached and according to the Council paper from January 2015, each part has different positions.

In such perspective, I will outline here both positions intended to show the impossibility of reaching an agreement following similar understandings and views.

The Council wishes to put under Member States responsibility the final decision on entities that should fall within the scope of the Directive. On the other hand, the Parliament has pushed forward a text that included a previous established list of entities and/or sectors that fall under the scope of the Directive. The main argument of the EP in supporting its approach is to prevent the possibility of MS excluding sectors/entities (or all) using the justification that the criteria established in the Directive is not met. (Council, 2015)

Moreover, it is the case that the EP desired a minimum harmonization also in respect with entities that fall under the scope, ensuring that such entities are identified in all MSs in the

same manner. On the other hand, the MSs work against a harmonisation in regards with the process of establishing entities which fall under the scope of the Directive, their view is that the aforementioned process should be of national competence. Nonetheless, the Council does not exclude adding within the Directive text safeguards, having in mind the following objectives:

- increase transparency of the process of establishing entities which fall under the scope of the Directive, at national level
- strengthen cooperation between MSs as to ensure comparable approach within the EU

Besides the tackled points, that concern the cooperation and scope issues, additional matters are to be discussed by the co-legislators, as for example elements *within article 14* (**Security Requirements and Incident Notification**) and *article 15* (**Implementation and Enforcement**).

4.4. Evolution of the Directive's text

Within this subchapter I will look upon the changes made in the directive's text and explain such changes in regards to the influence that it may have on Members States, on the European Union Institutions and as well as on the market operators that fall under this Directive's scope.

According to the Council of the EU (2015), the major issues in discussion between the co-legislators, the EP and the Council, are the scope of the Directive and the strategic and operational cooperation.

In this regard, changes in the scope will affect both Member States as well as market operators. Therefore, when looking at the text and the positions of the legislators' one has to have in mind the impact both on MS and the businesses that fall or not under the scope of the NIS Directive.

On the other hand, when talking about the cooperation network that is envisaged to be formed, one should look on the impact on both MS and also the European Union institutions

and their role. This can be argued as necessary given the fact that such cooperation takes place under the Union's umbrella and several Institutions are involved.

4.4.1. Changes that affect Member States

A first change MSs would like to obtain is within the subject matter of the Directive. The Council has therefore proposed an amendment to article 1(1) as it follows[22]: "*This Directive lays down measures to* ***seek to achieve and maintain*** *(****ensure****) a high common level of network and […]*". This amendment is consistent throughout the first article and following provisions, as it represents the MSs position towards the meaning of the NIS directive and what responsibility falls in the end on them.

By replacing the terminology, the subject of the Directive is diluted, within the Commission's proposed text "*ensure*" was meant to put pressure on MSs as they had to guarantee a high common level of security. On the other hand, if the Council text is pushed forward, MSs will only be responsible to the level of attempting to obtain a high common level of security.

Such changes in terminology can be noticed throughout the amendments proposed by the Council. Words meant to dilute the responsibilities of MSs are used instead of those preferred by the Commission and the EP. The terminology proposed by the Council, has not yet found approval from the EP, as a compromise is not illustrated on behalf of the EP within the Council's paper; just comments in several cases are put forward in the form of "*term is under discussion with the EP*". (Council 2015)

For the purpose of exemplification, bellow are presented such cases:

- Article 1 (2a) the word "**serious**" is added in order to qualify risks and incidents affecting network and information systems. The outcome of such change can, possibly, restrict the number of risk and incidents under the scope of the Directive; in the Commission proposal such word was not used.
- Article 1 (2b) the word "**ensure**", used by the Commission and the EP is to be changed with "**support and facilitate**" in regards with the cooperation between MSs that is envisaged to provide a forum for exchange of information and enhance

[22] In bold the new wording from the Council; in parenthesis ( ) appears the Commissions text

communication between MSs in regards with the risks and incidents affecting network and information systems.

- Article 14 (1) the word "**ensure**" used by the Commission and the EP is to be changed with "**require**" concerning the compensatory character of measures operators have to take in order to manage risks.

Moreover, within article 5 - National NIS strategy, the Council's text illustrates additional changes from the Commission and the EP's positions. The MSs would like to remove some of the provisions regarding the NIS strategy, thus having in the end the freedom to establish at national level such strategy without many pre-requirements. Some of the elements that would offer more freedom and in worst case scenario will dilute the effectiveness of the Directive are as follows:

- removing the requirements of the national NIS strategy to present the role and responsibilities of the government, article 5 (1b)
- removing the requirement to include a cooperation mechanism between public and private sector
- removing the requirement of a "***management framework to establish methodology for the identification, prioritisation, evaluation, prevention and treatment of risks and the impact of potential incidents***"[23]

Such dilution of the provisions of the Directive is put forwarded by the Council with the reasoning that Member States cannot on individual basis or within a collaboration network "*fully* ***ensure*** *a water proof level of NIS*" (Council, 2014b:3)

Moreover, changes supported by the MSs, target the establishment and the role of the national authorities and the single point of contact. Even if the EP agrees with the MSs desire to designate such role to an existing authorities, it wants to avoid conflict in implementation of the Directive. Thus, the EP has included within the text an exhaustive list of the type of authorities that cannot perform such task – [authorities that*]* ***"… does not fulfil any tasks in the fields of intelligence, law enforcement or defence and are not organisationally linked in any form to bodies active in those fields***"[24].

[23] EP's position as illustrated in Council, 2015, p. 35
[24] Ibid, p. 38

On the other hand, MSs do not agree with such text, as in some conditions the authorities prohibited by the EP's text to handle this role may be the only ones with capabilities and resources to do the job. Therefore, the MSs would find themselves in the need to restructure existing bodies, to invest in new personnel or to train existing one in order to perform the necessary tasks. An example in this case, is the situation of Romania, where the government has pushed forward for the Parliament's approval a cyber security law that empowered the secret service authority to become the NCA, as established in the proposed Directive.

Additionally, within the proposed Directive, the Commission, supported subsequently by the EP, has established core responsibilities for the MSs in regards with the national authorities. These responsibilities envisage the need of MSs to ensure adequate resources:

- *article 6, point 3* - to monitor that the established authorities/single contact point receive notifications of incidents (was initial under point 4, same article)
- *article 6, new added point 4a* (by the EP) - to ensure that the responsible national authorities forward information regarding an incident if such incident "***… has a significant cross-border impact***"[25].

Within the Council agreement may be found only for *point 3* of the above mentioned article, as the MSs have decided to delete for the text pushed forward requirements under point 4 (to monitor that the established authorities/single contact point receive notifications of incidents).

In general, same positions are taken also regarding the MSs responsibilities regarding the establishment of CERT/CSIRT. To be noted that CERT (Computer Emergency Response Team) is the terminology used in the proposed Directive by the Commission and approved by the EP. On the other hand, when addressing the same body, the MSs would like to use the terminology CSIRT (Computer Security Incident Response Team). A reason behind the use of different terminology is that "*CERT is a registered EU trademark*" (Council, 2014b:4).

Other changes that arise from the Council internal negotiations are to be put in line with enhancement of national security. By adding new points to the text, MSs have the ultimate goal of enhancing protection over national issues and agree not to share sensible information within the cooperation group. This adding consist in the fact that the provisions of the

[25] Ibid, p. 42

Directive should be "***without prejudice to actions taken by Member States to safeguard their essential State functions […] or to protect information the disclosure of which they consider contrary to the essential interest of their security***" (Council, 2015:16).

This point is supported by several countries as it is stated also in previous documents from the Council. Within the Progress Report of the Council, dated May 2014, it is stated that the MSs "*affected by an incident should decide whether or not and to which extent relevant information should be shared while taking national security interests into consideration*" (Council, 2014b:4).

4.4.2. Changes that affect EU's institutions and the cooperation between MSs and EU's institutions

In terms of the cooperation between EU's Member States, as mentioned before, the proposed Directive outcome is to establish a cooperation network. However, the Council has proposed the establishment of a cooperation group together with a CSIRTs network, keeping the same provisions as for the cooperation network, with some changes that will transform the group into a dialog platform. This differs from the EP's vision to have "***work programmes including action to be undertaken to implement the objectives and tasks***"[26]. Moreover, the EP asks for a report on the cooperation pursued within the NIS Directive to be examined by the EP, the Council and the Commission.

In relation with the CSIRTs network, the MSs want the possibility to refuse cooperation on the argument of national security, however the Commission and the EP are in opposition with such provisions. Moreover, the EP requests for annual assessment of the experience gained in order to use as an incentive to increase cooperation within the network.

EC acknowledge that information regarding NIS incidents is valuable to the public and business and that, sometimes, the respective information is available at national level online. Additionally, the cross-border business developments and the usage of online services, both for the wide public and from businesses, have to be taken into consideration. Thus, the EC argues that *"information on incidents should be provided in an aggregated form at EU level*" (Council, 2015:71), given the already existing cases that this information is available at

[26] EP's position as presented in Council, 2015, p. 61

national level and the importance of public knowledge. The Commission's proposal is that the secretariat of the CIRST network[27] has to maintain a website and put at the public's disposition general information regarding the major NIS incidents.

Additionally, the EP disagrees with the position taken by the Council concerning the rules of functioning of CSIRTs network. If the MSs favour a cooperation within the CSIRTs network by "***own rules of procedure***" (Council, 2015:76), the EP's text in *article 8b (5)* empowers the European Commission to adopt acts that regulates the functioning of the network.

Besides the changes in terms of cooperation, that to some extent does not affect to a large extent the role of the EU's institutions – the Commission and the European Parliament, changes desired by the Council in regards with the Commission's role within several areas of the NIS Directive are of a greater impact.

In order to illustrate the decrease of the Commission's role within the implementation of the Directive, changes in *article 5 (3)* can be brought to discussion. If initially, the Commission was to receive notification of the adoption and the content of the national NIS strategy within a month from the adoption, the MSs want only a summary to be available to the EU institution. However, such change is not supported by the EP, which has only agreed to an increase of the deadline to three months. The compromise sought further by the Council is to provide elements that cover parts of the Directive, without a list of actors involved in the implementation of the national NIS strategy.

Other points that illustrate the decrease of the Commission's role is the position of MSs within article *8b point 5* (**CSIRTs network**) and *article 16 point 2* (**Standardization**). As explained above, within *8b (5)* the MSs would like to remove the Commission's capacity of pushing forward acts to regulate the functioning of the CSIRTs networks. Similar change is desired also in regards to the role of the Commission in elaborating a list of standards in order to assure a convergent implementation of the requirements under *article 14 (1)*. To this extent, the Council may agree on the elaboration of recommendations and guidelines by ENISA in collaboration with the MSs, motivating the need for considering national standards that already exist.

[27] as specified in the Directive's text this function is to be provided by ENISA

Such changes in the text, not only diminishes the Commission's role, but can also have a negative impact in the Directive implementation in the sense that a standardization will be harder to achieve if each state elaborates its own standards. A negative impact may also occur on operators that provide services in more than one Member State, if standards differ between those states.

4.4.3. Changes that affect market operators

Firstly, a clarification is needed in the fact that stakeholders, as addressed before, are the market operators that fall under the scope of the directive. Taking into account their lobby capacity and the different positions that resulted upon the publication of the Directive, at EU level, is to be believed that these operators influence at national level the position of MS.

Taking the aforementioned as a departure point, I will look into the changes the Council proposes in terms of scope and provisions for operators (responsibilities and requirements) to illustrate the influence of such operators at state level. Since the reason for changes of those elements cannot exhaustively be connected to interest group influence, I will also take into consideration reasons that may belong purely to State level.

A first amendment put forward by the Council, in regards to the operators, is within article 3. Within this article it is stated the definition of an operator, as per MSs understanding – "***a public or a private entity, which provides an essential service in the fields of Internet infrastructure and digital service platforms, energy, transport, banking, stock exchanges and health and water supply***" (Council 20015:26). This does not differ much from the definition put forward by the Commission in its original text and by the EP's approved text. However, the difference comes in the fact that the providers listed above have to fulfil certain criteria to be included in the scope of the directive. Moreover, the Council's new text stipulates that every MS should identify private entities that fall under the scope of the directive, that meet the criteria established within the definition of the operators, in the Directive's text. Such criteria are:

- the dependence on network and information systems of the service has to be to a large extent;
- an incident on the network and information systems of the service has to have an important disruptive effect of the service or on public safety.

Thus, one can affirm that such position of the Member States can be explained by two points.

First, it can be the reason of national power, and the desire of MSs to establish their own provisions. However, this comes with a considerable negative effect; the harmonization in this area will be affected as the operators identified in some MSs will be out of the scope of the directive in others.

Secondly, the changes can be explained in regards to the position of interest groups, namely the operators that may fall under the scope of the Directive. Using their lobbying power and motivated by the financial aspects of needing to create a secure system within, operators can influence national governments to push for their own agenda at EU negotiations.

For example, the lobbyist group that includes companies like Facebook, Microsoft and Google supports such changes as it implies compliance costs. "*Online services such as e-commerce sites, search and social networks are useful but not critical. This legislation should focus on truly critical infrastructure only,*" states James Waterworth, the vice-president for Europe of the Computer and Communications Industry Association. (Reuters.com, 2014)

As shown from the impact assessments, implementing the Directive's provision can be costly and the fact that, as Council proposes, MSs have the capacity to name operators that fall under the scope of the directive can be to some extent used in favour of some stakeholders. Operators from Eastern countries and those from fragile economies, such as Greece, where the law can be to some extent influenced by power, can benefit from such changes. Players in the private sector from Western and Scandinavian countries share such views, also. Rasmus Theede, CISO at KMD (Denmark) puts under question the effectiveness of the Directive given the different approaches to security within the MSs of the Union, starting to doubt the possibility of a unified level of security. Thus, Theede takes a personal stand: "*I personally think that is a utopia to think that the countries of Scandinavia, which generally have a high level of IT security, and countries such as Greece, Portugal and Spain, which are all dealing with other severe economic issues, are all going to participate in a strong IT security cooperation*" (Dinesen & Saether, 2013:59).

Additional changes, that can reflect influence from stakeholders, are to be found in *article 14* (**Security Requirements and Incident Notification**), where besides the change of wording in regards with the MSs responsibilities, the Council's text also present differences from the

version supported by the EP. In this regard, the MSs are only to request from operators measures to manage risks, but not to monitor if the operators in question implement such measures, as the Commission proposes and EP supports. Thus, it can be the case that an interest group pressures national governments to lower their monitoring, but not being subject to control by authorities. In some cases, these can be motivated by the possibility of imposing over requirements, thus in order not to fall in the other extreme the easiest way is chosen. Moreover, as the Council text shows, operators are not obliged to take measures that "***ensure a level of network and information security appropriate to the risk presented***" (EP's position; Council, 2015:94-95), but those measures should maintain a level of security.

Lobby on behalf of operators can be seen also in the EP's amendments and it has repealed the Commissions power to adopt acts in order to establish the circumstances in which operators have to notify incidents and such power was passed to the MSs. However, such influence of the operators at the national level is higher, as within the Council position such provision can be accepted, in the condition of request from the operators of such guidelines. Therefore, the MSs are more interested in a voluntary approach and operators are left to decide what and when to report, without clear guidelines besides the Directive text that will be transposed into national legislation following its adoption (Council, 2015).

Another important change, is the wish of MSs to retrieve the obligation of operators to be subject to a **security audit** and share results with the competent authority - *article 15 (2b)*. The provision of security audit, put forward by the Commission and sustained by the EP, will have a financial impact on the operators. However, at the same time, it will ensure the good translation of the requirements and will assure the beneficiary of their services the state of art protection of their data and stability in accessing/being provided the service.

Moreover, *point 3* of the abovementioned article, envisages that the competent authorities at MS level will issue binding instructions to operators in terms of NIS. Following discussion in the Council, this point was amended as it follows "***the competent authorities may issue instructions to the operators to remedy their operations***" (Council, 2015:113). Thus the operators are not to be obliged to remedy their security provisions. Such alteration, may risk the inefficiency of the directive, if the operators actions are left on a voluntary basis, thus, harmonization can be achieved with greater effort.

An example of the pressure coming from the private sector to diminish the impact of the Directive can to be considered the paper pushed forward by DIGITALEUROPE. The group represents the digital technology industry in Europe, with members that include some of the worlds largest IT, telecom and consumer electronics companies and national associations from Europe. A presentation of the group, its members and national representatives within MSs are to be found in Annex 4.

Within the paper expressing the group position regarding the NIS Directive, it is stated "*that market operators should be able to make use of self-compliance mechanisms to demonstrate compliance as opposed to competent authorities undertaking audits*" (DIGITALEUROPE, 2013). They consider that companies that are located in several MSs will undergo a significant administrative burden by having to work with several competent authorities to conduct the necessary audits.

Harmonization, in terms of cyber security, is necessary for the standing point of One Single Market within the EU countries, as companies nowadays have extended their businesses beyond borders of one MS. In this regards, Jacqueline Johnson, head of IT Security at Nordea Bank acknowledges that "*there is an interest in being able to store information in other countries than in Scandinavia, Germany, England and France. We need to have some sort of guarantee for the security when considering this and therefore try to have some sort of minimum level across the EU*" (Dinesen & Saether, 2013:57).

***

After illustrating some of the changes that affect operators within the scope of the Directive and based on the fact that such scope is yet to be agreed between the EU co-legislators, it makes sense to incline towards a significant influence of the stakeholders within national states. This can be put forward given the Council's position to push towards a voluntary participation of operators and to offer the MSs the ability to decide what to apply and to whom. On the other side, the Commission, when proposing the legislation, and the EP following its approval, take a different stand, requiring clear delimitations for operators within the Directive's text and a regulatory approach.

Same as Member States, companies argue that EU's role should be kept limited in terms of interfering in national, respective companies matters. Thus, the EU should promote

improvements of cyber security, but the extent to which the EU could get involved in the companies' operations should be somehow limited.

Following a stakeholder consultation within the UK's Government (2013) on the issues of the proposed Cyber Directive can be understood that the overall preference is for a voluntary, non-regulatory approach. To this extent one stakeholder declares that *"…the existing non-regulatory approach in the UK can help to promote open and transparent engagement between businesses and government… this has facilitated a secure and effective environment for sharing information. We think that the systems and processes laid out in the draft Directive could create additional costs with no material security or resilience benefit*" (UK' Government, 2013:24)

On the other hand, some actors would agree to a clear legislation at state level. According to Henning Mortensen on behalf of the Confederation of Danish Industry, "*the security responsibility is placed with the companies and that is the way it should be. The legislation could be specified by the states on what the companies should do [...]. The responsibility should be with the companies*" (Dinesen & Saether, 2013:60). It is not to be understood that the Danish operators would rather have a regulatory approach, as such data could not be obtained, but to some extent they could accept regulations within national law.

4.5. Member States position

Within this part of the case study I will look upon identifying the divergence in opinions of the Member States. As per different sources, it is known that within the Council an agreement has not been reached in many areas, due to different opinions of the MSs.

This year, the Latvian Presidency of the European Council has been pushing the Directive as part of its portfolio relating to the European Commission's Digital Single Market plans, as it happened last year during the Italian presidency. Following declarations, at a cyber security conference, cited by EurActiv.com, it appears that after the informal trilogue meetings that took place in the last part of 2014 and the beginning of 2015 between the EP, the Commission and the Council, there are still issues to be debated and compromise is not considered.

"*I came in thinking we'll try to finish the directive by the end of the presidency. At some points I felt desperate. [..] This is the first EU regulation and we're not able to compromise. […] It doesn't give a very powerful message to those we're going to confront*"
Jānis Sārts, State Secretary of the Latvian Ministry of Defence, 28 May 2015

It has been reported that agreement has not been reached between the MSs in regards with the mandatory reporting clause. Some Member States such as Ireland, Sweden and the UK oppose the provision of requiring reports of cyber attacks to large non-European companies. At the same time, there are states that oppose the mandatory reporting altogether, as for example France, Germany and Spain. (EurActiv, May 2015) Countries, such as UK, that have already implemented a voluntary system for reporting, take the side of the soft power approach when it comes to collecting reports for security breaches. Same point is put forward by the private sector lobby and companies within states.

On one side, MSs push against the mandatory reporting arguing that the burden on the companies will work against the resilience sought, as an officer within the UK Department for Business, Innovation & Skills declares "*Smaller companies in particular, they might just stop looking for violations. That would be a massive disincentive to the kind of higher resilience we're trying to do*". (EurActiv, May 2015) On the other side, EU's officials fear that a voluntary basis for reporting will translate into a weak cooperation.

Other issues that are still debated within the Council, as MSs take different positions, is the scope of the Directive, and more precisely which businesses are to be included within the scope of the Directive's requirements and the fact that member states see digital security as a national issue and would like to act accordingly.

Therefore, on this aspect, EU member states that host US-based internet companies, as it is the case of Ireland, Sweden and the UK, are working against the involvement of such companies. On the other hand countries like France, Germany and Spain are opposed to the idea of excluding such companies from the Directive's scope. A possible compromise has been reached within the Council in this regard as some MSs, like is the case of Germany and the UK, prefer to leave the choice of business at national level.

"*For the Council it is important that the scope of this Directive focuses on those businesses that provide critical services on whose networks a cyber-incident would cause major*

disruption to society or the economy. Furthermore, it is only Member States that are in the position to identify these businesses at a national level. Retaining these two principles within the text is of utmost importance to the UK Government."[28] This reading is part of the correspondence within the UK Government and the UK representative working group at EU level and it illustrated, besides the UK position also the fact that MSs have reached a consensus in terms of the scope of the Directive and in their capability of identifying at national level businesses that fall under the Directive's requirements.

At EU level the position is on the opposite side, as the EP fears that national capabilities in determining businesses that fall under the scope of the Directive might leave some states with an empty list. Others think that there is an issue of mistrust between MSs and therefore this reluctance of cooperation and giving up a sovereign power. Supporting this, Peter Round Director of Capability, Armament and Technology within the European Defence Agency thinks that "*One of the issues with cyber is that it is in some ways the new gunpowder. When a member state gains a capability – certainly at first – they don't want to share it, because some have it and some don't, and we are seeing that some don't want to share it, seeing it as a sovereign and national issue*". (EurActiv, April 2015)

[28]28 January 2015, Letter from Edward Vaizey to the Chair (in regard with the NIS Directive discussions)

V. Analysis –the NIS Directive and the decision making process in the EU

Within this chapter, I will proceed in identifying the most appropriate hypothesis, resulted from the theoretical framework and the empirical data, which can explain the changes in the directive and the relation between the EU institutions and the Member States. In other words it will be a discussion of how the changes reflect of the theory and more precisely from what point of view one should look into the decision making process within the cyber security policy making in order to identify the nature of holdbacks within.

Thus, the first subchapters will contain analysis of the changes and interactions outlined in the case study chapter in relation with each of the theories previously illustrated and the hypothesis identified. Following, a discussion part will connect the policy making modes illustrated in the theoretical part with the findings and remarks regarding the intensity of interest in connection with cyber security will be outlined.

5.1. Predominantly of intergovernmentalism influence?

The first hypothesis that I intend to analyse, in connection to the negotiations within the approval of the NIS Directive, refers to the intergovernmentalism approach towards decision making.

The analysis of this first hypothesis assumes a deep understanding of the EU's intergovernmentalism aspect and the changes that can be traced back to EU MSs interest and preferences. Although it is clear that the EU is trying to promote the single market through a standardised system of laws that apply in all member states, some areas are still under MSs decision making powers and to some extent it is preferred to remain so.

Consequently, in this first part of the analysis I intend to scrutinize particularly on this aspect; and in doing so I will support the analysis on the liberal intergovernmentalism view that the decision making process comes following a series of intergovernmental bargains, each MSs supporting its position that results from a cost benefit analysis and the pressure of national preferences.

This first section will explore the changes within the proposed Directive that can be traced back to MSs interests and pressures from stakeholders. It will research the extent to which one can consider viable enough the idea that MSs are the one to direct the policy outcomes and policy harmonization in the EU.

Considering the above, the first step in determining if the MSs are the ones merely responsible for the decision making process and policy harmonization is to look at the MSs position and the changes within the Directive text that affect the MSs. Additionally, the influence and the changes that affect market operators and their position and influence have to be included. All these elements are to be put in correlation with the cost and benefits of the proposed Directive in order to assess if the liberal intergovernmentalism approach to decision making is applicable to the problem at hand.

Cost and benefit of interdependence

Following Moravcsik's thought there is a cost and benefit variable that governments take into consideration when deciding to collaborate in supranational institutions.

The costs are not merely covering the financial aspect of the collaboration, but also the loss of national power, aspect that will be dealt with in connection with MSs influence in negotiations.

In regards with the financial aspect, as shown in the impact assessment part, there are several costs that will come and burden the MSs budget in order to comply with the requirements of the NIS Directive. These costs will affect to some extent all MSs, depending on their level of development in regards to cyber security.

The proposed Directive has an extensive reach and MSs will be obliged to commit important resources in order to comply with the requirements. There are only few states that have a developed legal and institutional framework to handle cyber security issues, thus they will be required to invest less in order to reach the EU required level. This might be the case for states like Germany, France, Austria and UK; but the extend of the resources needed will depend on the final requirements, as some of them are adopting in their national strategy a voluntary approach, in opposition with the proposed Directive, which has a regulatory approach.

It is also the case of states without a developed national strategy and adequate institutional framework. Some states, such as Greece, Ireland, are in the situation of not having created national CERTs. For these states the necessary of resources will be exponentially bigger. Only the cost of creating a CERT is estimated to 2.5 million EUR. To this initial cost it is also added the need of human resources that will undertake the tasks for managing national authorities and collaborating with private sector.

An additional burden is to create a secure network for sharing incident reports and relevant information between national authorities. This has been estimated at around 10 million EUR each year.

A positive aspect is that part of these costs are to be supported by the EU budget. On the other hand changes within the Directive text come to moderate the financial burden. Such changes are in connection with restricting the number of operators that fall under the scope of the Directive, implementing the cooperation network following their own rules and assessment. Therefore, the overall financial impact might be leaner that previsioned given the changes MSs would like to make to the Directive.

Pressure of domestic groups

It is commonly accepted that stakeholders will try to influence decision making through lobby in regards to different policy aspects. Within the process of proposal of a NIS Directive, consultations were held by the Commission in order to push forward a comprehensive document, corresponding with the reality in the field.

Following the publication of the Directive, many lobby groups and companies have offered their perspective in what should be included and not within the Directive text. As evidentiated in the empirical data part, companies that may be targeted by the proposed Directive are trying to influence decision makers.

A first point is their inclusion within the scope of the Directive, where internet enablers, e-commerce platforms, social media platforms, etc. are arguing that they are not critical operators/providers and require to be excluded from the reach of the NIS Directive. Identified, is the position of states that agree with this exclusion, states like UK and Sweden

that host such companies, therefore the influence of pressure group at national level becomes clear.

Another point that is connected with the influence of companies is within the provision of audit that operators have to undergo, as per the Commission and EP's text.

Lobbing groups are arguing that a self-monitoring system would be enough and the requirement of security audit should be removed (DIGITALEUROPE, 2013). Accordingly, MSs assess that such requirement is unnecessary, additionally proposing that national authorities should give only recommendations for companies to remedy their failure in case of attacks, not binding requirements as established by the Commission.

Such changes come in line with the idea of financial burden that will affect all operators that fall under the scope of the Directive. It has been assessed that companies, depending on their business size, will have to spend between 4 000 EUR and 50 000 EUR annually to comply with the NIS requirements. The financial impact of the Directive is to be put in connection with the market operators' influence upon national governments. Thus, as shown, companies are using their capabilities to influence national governments position either for exclusion or for dilution of the impact on businesses.

Bargaining in pursuing states interest

As stated, MSs encounter, also the cost of losing national powers in favour of a supranational cooperation.

The European integration process has shown that it takes time for MSs to give up their capabilities; therefore, when entering into a new area of cooperation at EU level, MSs are trying to protect their national power in the field and to push their own interest, as seen from the data put forward.

In many areas, the Council, therefore the MSs have adopted a different position that the one of the Commission and the EP. From the small changes in terminology that have the overall effect of reducing their responsibilities, to the inclusion of provisions that might hinder cooperation, MSs have tried to push forward their own view and interest.

Of major importance are changes that envisage MSs capability of identifying businesses at national level that fall under the scope of the Directive. "*For the Council it is important that the scope of this Directive focuses on those businesses that provide critical services on whose networks a cyber-incident would cause major disruption to society or the economy. Furthermore, it is only Member States that are in the position to identify these businesses at a national level*."(UK Government, 2015) Besides ensuring their capability to decide to whom the directive should apply to, MSs would also like to decide to what extent information regarding a cyber-incident will be shared within the cooperation network. (Council 2014b) Such changes will affect cooperation in the field and will translate into fragmented internal market. MSs will continue in some areas to work on their own and differences in implementation of the Directive between states may hinder business progress.

In addition, new text put forward by the Council assumes that MSs will be in the capacity to decide the cooperation methods and ENISA will support them, excluding in this way the Commission for involvement.

Within the progress reports published by the Council it appears that MSs position is similar in a large extent, negotiations took place in regards to the operators that are to be included in the Directive. However, a common agreement was put forward; as shown above, MSs will like to take this decision at national level. Interstate negotiation in order to push forward own preferences it is assumed to have taken place before hand, however, as shown for the available data, major discrepancies in views are in relation with the regulatory mode vs voluntary approach. Moreover, measures towards "lighting" of the regulatory approach have been taken, as for example the removal of the safety audit companies who were supposed to make evidence for. Thus one can conclude that to some extent the negotiations between governments have had positive results and as per Moravcsik's view, the benefit of cooperating at supranational level was translated into following such cooperation according to own interests.

The overall approval process seems to be a bargaining operation between the EU institutions and the MSs, reunited in the Council. The Member States are trying to protect their national powers and interest and the EU institutions are working towards harmonization in the cyber security field at EU level.

***

The hypothesis that the decision making process is predominantly of intergovernmentalism influence applies to the negotiations for approval of the NIS Directive. As explained in the theory chapter, liberal intergovernmentalism illustrates the European integration as a process of domestic formation of nation preferences, intergovernmental bargaining in order to reach agreement and creation of institutions at supranational level as to secure such agreement.

Within the context of the approval of a NIS Directive at EU level, even if the Directive was pushed forward by the EU Commission, the formation of domestic preferences and the bargaining are vividly present.

Changes made within the text, at Council level, together with the information provided by the progress reports that illustrates different positions of the MSs, shows that, the intergovernmental bargaining that takes place focuses on national interest and, as shown, changes reflect such interests. Changes in term of collaboration at EU level and regarding the reporting of progress support the intergovernmental approach.

The primary determinants of national preferences, as put forward by the LI, are to be the cost and benefits of economic interdependence. In this regards the benefits for policy harmonization are to be measured in comparison with the financial and national power costs. Following, the pressure of national groups is here translated into influences of stakeholders/market operators, motivated by the financial costs, to obtain a favourable legal framework.

5.2. The EU institutions - key players within the decision making process?

This section aims to investigate on the plausibility of the second hypothesis formulated in this paper, namely that the ***EU institutions are the key players within the decision making process***. In doing so, I intend to use the institutionalism theory and the constructivist approach to explain/backup the idea that the EU institutions influence the preference formation and decision making.

According to the theoretical framework, institutions shape the behaviour of actors within them and, in such case, decisions are taken within working groups, at supranational level. Following such approach one would discover that policy making is generally happening in Brussels, as national representatives come to interact and exchange agreements in order to push forward policies.

Thus, in order to demonstrate the reality of such affirmation, I would look upon the role of the EU's institutions, mostly the EC and the EP, in the negotiation process for the approval of the NIS Directive. Changes that affect EU's institutions and the collaboration at EU level are to be brought into discussion. Moreover, the theories are to be used in connection with the data available to identify the socialization aspects that are underpinned to institutions and how they affect the policy harmonization process.

A first point that can be related to the theoretical perspective of institutionalism is the ideology upon which the cyber security Strategy and the NIS Directive was put forward – "*to further European values of freedom and democracy and ensure the digital economy can safely grow*" (Commission Press release, 2013). In addition, the Commission's capability of putting forward such legal framework is based on existing EU treaties and takes into account EU's principals, such as the subsidiarity principle.

However, one can affirm that this is not convincing evidence, if this is all there is. The Commission is empowered to operate by the EU's treaties, but with each piece of legislation set forward it has to be shown that the MSs have previously conferred the power undertaken in the field or not. Therefore, the evidence of existing norms and ideologies that are reinforced within the EU institutions is not enough, given the fact that states do not act automatically according to them. Moreover, the fact that the Council takes its stand following bargaining between MSs and not according the already promoted EU's values and adopted treaties comes in opposition with the institutionalism view.

A second point that can be raised in supporting this hypothesis is the existence of formal and informal meetings that take place within the process of approval. The working groups and especially the meetings in COREPER are, according to institutionalists, important forums of mind setting.

Within the constructivist approach, theoreticians attached to supranational institutions the power of changing identities and beliefs towards the sense of community. In this regard, within the approval process of the NIS directive one can identify the existence of working groups, some created in order to find consensus, as it is the trilogue informal meetings between the EU's legislators.

However, common policy commitments have not resulted yet, as seen in some areas MSs are grouped towards opposed preferences and to some extent all prefer to commit on their own. This is the case with the involvement of internet companies within the scope of the Directive. Some states, such as Ireland, Sweden and UK are opposed to such involvement and on the other hand France, Germany and Spain would like to include them.

A common ground has been found, however, this does not come in line with the EU view, MSs preferring to take from supranational level the ability to decide what operators are involved and make this a national matter.

Thus, taking such developments into account, it is hard to support the idea that interacting within supranational institutions has made national representatives to change preferences. Major agreements have not been established. Moreover, following the work in these informal groups, consensus was not found in the important areas, as scope of the directive and operators involved. As shown in progress reports (Council 2014, Council 2015) the EP and the Commission are on opposite sides from the Council, thus the Member States, therefore identities and beliefs were not affected by such collaboration.

It is possible that one can argue that given the position taken within this process by the EP, socialization and transformation of beliefs to actually take place within institutions. However, I here take a different stand. It is actually comprehensible that the EP has different perspectives as from the ones of the national governments, in the sense of supporting a more European path. EP members are elected by citizens to represent their interests at EU level; therefore their ideology is in line with the party ideology. A general support for national interest it is wrong to be found within the EP, as that will mean a failure within the overall democracy concept.

Another point that plays against an assessment of institutions as the mere players within EU decision making is the Council's approach in regards with the Commissions capabilities and

role within the cooperation framework and overall cyber security directive implementation. If in the original text and further in the EP's approved text, the EU Commission was empowered to adopt acts that regulated the cooperation between national CERT in order to ensure a unified framework, The Council wants a cooperation within national entities following MSs own procedures and standards. If the final wording will respect the Council's views it will be the case that the EU institutions role will be diminished and what was viewed as a supranational cooperation framework would be therefore hindered by national interests.

However, it is to agree that the EU institutions come to constraint national governments to take measures within the cyber security field. To some extent this comes in line with North's perspective of institutions, as pressure for political action. As shown within the empirical data and as seen in Annex 2, not all EU countries have taken action in the field of cyber security. The entry in force of an EU directive in the field will come to constraint governments to undertake serious action in this regards and will incite others to do more in assuring a safe cyber environment.

***

As seen until now, in regards with the examined process, the idea that institutions are the key players in the policy harmonization in the field of cyber security within the EU does not illustrate the findings. Elements that are directly connected to the institutionalists and constructivist view cannot be connected with the data presented in the paper in the view that institutions create policies and legal frameworks in the cyber security area and national actors fall under the socialization effects of such institutions.

However, an indication of the influence of the institution comes from the fact that strategies adopted at EU level are translated in national legislation by governments. As shown by Pierson (1996), actors may be in strong position initially, but undertaking different reform in order to commit to the supranational strategies they come to their position.

Thus, it is to assume that given the fact that the cyber security field is a new area of interest and a new sector of capabilities at EU level, it is natural that national powers are not easily transferred to supranational institutions. However, following the institutionalists' view, with time EU's institutions will develop into key players, as is the case with other policy areas, such as agriculture, commercial, environment, etc.

5.3. Discussion

Together with the proposed EU data protection regulation, the NIS Directive, once adopted, will have an important impact on many public bodies and businesses. For the first time in the EU, there will be an information security regulatory framework with national authorities and European-wide information security standards.

The NIS Directive will also require many businesses to apply procedures that will demonstrate effective use of security policies and measures. Failure to do so may result not only in loss of customer trust and damage to reputation, but also breach of the European data protection and information security requirements and enforcement actions.

The EU Member States have managed to agree, to some extent, to changes that come to provide more national capabilities and to hinder, to some extent harmonization. Put under the sign of protection of national interests, cooperation at EU level has to be regulated in terms of own assessment.

Moreover, MSs are searching to restrict further the role of the Commission. As shown, the original text provide the Commission with notifications and contents of national strategies, however, MSs want to restrict the access of the EU institutions and they propose only to provide some elements of its content, without a list of national actors that are empowered to implement it. This will result in a fragmented overall image of the EU cyber security actions.

However, the purpose of this paper is not to assess the quality and the reach of what is yet to be put forward as the EU's Network and Information Security Directive. I undertook this documentary research in order to find the major influences of decision-making within the approval process of the above-mentioned directive, or yet, better said the lack of decision making.

The EU policy making

After identifying that within the approval process of the NIS Directive, MSs have much more influence then EU institutions, thus the intergovernmental approach describes better the process. Now, it is left to assess what policy making mode fits the process.

Even at the first glance one can exclude the *Policy Coordination and Benchmarking mode* and the *Intensive Transgovernmentalism*.

For the first one it is easy to see that within the process of adopting the proposed NIS Directive negotiation is the most prominent procedure; transfer of ideas and techniques from the MSs that have already developed extensive national strategies is not used. Even if this approach is characterised by the intergovernmental cooperation, an important aspect is the supranational character. Overall, this mode assumes an extensive cooperation at EU level and is translated by theoreticians, such as Wallace (2000) as being the promoter of Europeanization.

I have also excluded *Intensive Transgovernmentalism*, as it explains policy making without much involvement of EU institutions. As shown in the theory chapter, there are special mechanisms in place to support the cooperation that is conducted by the Council. This is not the case of the Cyber Security Strategy as within the approval process of the Directive Trilogue meetings took place and stakeholders were invited to public consultations.

Following the above assessment, the *Distinctive Community method* and the *EU Regulatory mode* are left. As it results from the presented data and the analysis undertaken before, within this decision making process one has to exclude the Distinctive Community method and agree that the EU regulatory mode fits best.

First, I will motivate the exclusion of the *Community method*, even if at first glance it may seem to be more appropriate given the fact that the process under which the NIS Directive was proposed is similar to the one described by Wallace (2006). The EC proposes the directive, the Council has as co-decision partner the EP, and votes in the Council are obtained through bargaining. However, this is not the case here, as until this point MSs are working towards minimum standards of harmonization and national powers in mostly all issues encompassed within the Directive.

The *regulatory mode* is to be found as a better explanatory for the current situation. Such mode of policy making describes the negotiations for the NIS Directive. The Commission has put forward, following expert and stakeholder consultations a comprehensive Cyber Security Strategy and a NIS Directive that has the purpose to set minimum standards in the sector. Throughout a co-decision procedure, the EP and the Council are to adopt the legal

framework; however, the EP has limited power in negotiating with the MSs; MSs that support including their national preferences in the text and agree on a minimum level of harmonization; even if not all member states want a regulatory approach to the cyber security issue.

This comes to describe very well the on-going process of negotiation, where even with different perspectives on several issues; MSs are easy to find compromise by including those under national capability. As it is the case, the EP's view is different and within the negotiations, it has been shown that compromise can be achieved, more in favour of the Council. Evidence stands the fact that the EP has agreed to remove a number of provisions just to obtain flexibility in terms of the scope of the Directive from the Council; however, until this point a common stand has not been reached, given the fact that the Council view is opposed to the one assumed by the EP.

Salience

The concept of salience is brought here as the intensity or importance of the interest that MSs attach to the cyber security issue.

As no progress is yet visible within the approval process, one can affirm that the interest MSs pin on cyber security issues is not quite of high intensity; therefore, the aspect of security of cyberspace is not important within their national policy. This position will be entirely wrong.

Following Coleman's (1990) and Konning & Proksh's (2006) line of thought, the EU member states have attached a high salience to the cyber security issue and thus to the NIS Directive, given their effort in defending their stand. As shown, the changes within the Directive's text illustrate the MSs efforts in maintaining their national capabilities in the field and pushing forward their views of handling this issue. The extensive negotiations meeting confirm the fact that MSs have put significant resources into this issue.

The data confirms the finding of Leuffen, Malang and Worle (2014), that salience in decision making is strongly connected with preferences and interest and not with power. Thus as it is the case of the Council, therefore the MSs, attaching a significant importance to negotiations and bargaining to push forward own text translates into a high intensity of interest in the field.

As discovered from the data, high level of salience is to be attached also to the EU's position in regards with cyber security. Throughout discourse, EU officials are trying to support their approach and interests and, at the same time, stress the importance of the cyber security directive. "*For cyberspace to remain open and free, the same norms, principles, and values that we uphold offline must also apply online*" Catherine Asthon declared within the press conference following the publication of the European Union Cyber Security Strategy (Hammond, February 2013:3). Moreover, within the EU's Cyber Security Strategy it is expressed the need of the EU and its MSs for a strong and effective legislation in the field. (European Commission, 2013c)

Same interest can be observed also in the private sector. The manager of IT Security at Nordea Bank Denmark declares - "*We need to have some sort of guarantee for the security when considering […] try to have some sort of minimum level across the EU*" (Dinesen & Saether, 2013:57). Therefore, it has come to that point that given the free movement across the EU, there comes the necessity for businesses that want to internationalize in other EU countries to have a guarantee of security in order to expend their business.

VI. Conclusion

As showed and discussed in this paper, the EU is trying to pushed forward a common Cyber Security Strategy and the NIS Directive that will increase the resilience to cyber attacks. Together with other legal frameworks, this comes to support the EU's approach towards cybercrime and the common market.

However, regardless of the necessity of action in the field, the increasing number of cyber threats and the danger related to the ICT sector, the EU's approach is not translated into action due to delay in approval of the above mentioned Directive. The negotiation process, started in 2013 following the publication of the NIS Directive by the EC has not ended yet.

Thus, the legitimate question to ask in these conditions is "***What could be the nature of the holdbacks in agreeing on a common cyber security policy in the EU?***".

In answering this question, I have first looked upon the theoretical approaches that relates to the decision making and policy making at European level. Using Moravcsik's liberal institutionalism, the constructivism and new institutionalism views, but also the salience theory I have put forward a series of variables that affect the decision making process. Following the same pattern, I have identified two hypotheses that can be put in relation with the intensity of influence of these variables within a decision making process.

Moving forward, within the empirical part, I have looked upon the content of the NIS Directive and its approval process. For a better understanding of the situation, changes within the proposed Directive content have been identified and correlated with elements that they affect.

Putting the empirical data in connection with the theoretical framework from the beginning made it easier for the analysis part. Following the hypotheses identified in the first part of the paper, I have discovered that the process of approval of the cyber security Directive is influenced mostly by the MSs. The role of the EU institutions within the process is limited.

As shown, the MSs are trying to limit as much as possible the Commission's powers within the proposed framework. On the other hand, the Parliament is giving up to MSs pressures, excluding provisions of the text in order to obtain compromise of the Council in areas that until this point MSs want expressly to keep under national powers.

Thus, when it comes to pointing out the nature of holdbacks in policy harmonization within the field of cyber security at EU level the most significant impact comes from the MSs. Even if in some areas, cooperation at EU level has moved forward and the EU, through the Community method imposes cooperation, there are still areas, even under the community umbrella in which cooperation is hard to be obtained.

I have discovered that within the process, the regulatory mode of policy making applies, even if the Commission is the one that proposes the legislation, and the Parliament is co-legislator, throughout intergovernmental bargaining MSs manage to impose their national preferences.

My findings show that the process of decision making in EU is complex and no single theory can comprehend the multitude of relations and interactions that take place, especially in sensitive areas like cyber security. Further research could target other decision making process in similar fields in order to assess if the pattern is kept, or if in other cases MSs are more willing to cooperate.

However, given the fact that this is an on - going process, upon the approval of the Directive patterns might change. If that will not be the case in the end, the limited harmonization and fragmented approach towards cyber security will continue to characterize the European Union's strategy in the field.

Bibliography

Achen, C.H. (2006) *Institutional Realism and Bargaining Models*, In: Thomson R, Stokman FN, Achen CH and König T (eds) The European Union Decides. Cambridge: Cambridge University Press, 86-123.

Barett, M., Bedford, D., Skinner, E. & Vergles, E. (2011) *Assured Access to the Global Commons – Maritime Air Space Cyber*, NATO, Norfolk, Virginia

BSA The software Allince (2015) *EU Cybersecurity Dashboard - A Path to a Secure European Cyberspace* www.bsa.org/EUcybersecurity, accessed 06.02.2015

Bulmer, S.J. (1993) *The Governance of the European Union: A New Institutionalist Approach*, Journal of Public Policy, Vol. 13, No. 4, p. 351-380
http://www.jstor.org/stable/4007518, accessed 14/05/2015

Bulmer, S.J. (1998*) New institutionalism and the governance of the Single European Market*, Journal of European Public Policy, 5:3, 365-386

Checkel, J. (1998) *The Constructivist turn in International Relations Theory (A review Essay,)* World Politics, Vol. 50, No. 2, pp. 324-348
http://dx.doi.org/10.1080/135017698343875, accessed 10/05/2015

Christiansen, T. Jorgensen, K.E. Wiener, A. (1999) *The Social Construction of Europe*, Journal of European Public Policy, Vol. 6, No. 4, pp 525- 544

Council of the European Union (2013) *Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012109%202013%20INIT
accessed 03.04.2015

Council of the European Union (2013) *Progress Report - Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, Brussels, 22 November 2013
http://www.eerstekamer.nl/eu/documenteu/16630/13_voortgangsrapport_litouws/f=/vjf3mz6et6sq.pdf , accessed 12.03.2014

Council of the European Union (2014b) *Progress Report - Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, Brussels, 22 May 2014

http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010097%202014%20INIT accessed 12.03.2015

Council of the European Union (2014a) *Information on the state of play Report - Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, Brussels, 19 November 2014 http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015639%202014%20INIT accessed 12.03.2015

Council of the European Union (2014) *Preparation of the 2nd Informal Trilogue - Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, Brussels, 4 November 2014 https://www.yumpu.com/en/document/view/33760259/eu-council-nis-2nd-trilogue-14850-14 , accessed 14.03.2015

Council of the European Union (2015) *State of play and work ahead - Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, Brussels, 14 January 2015 http://www.statewatch.org/news/2015/jan/eu-council-NIS-5257-15.pdf , accessed 04.06.2015

DIGITALEUROPE (2013) *DIGITALEUROPE Comments on the Draft Network and Information Security Directive* http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=566&PortalId=0&TabId=353 , accessed 12.04.2015

Dinesen, S.L. & Saether, H.B. (2013) *Cyber Security – Securitizing cyber threats in Denmark*, Copenhagen Business School

Donck, F. (2014) *ISOC European Regional Bureau Newsletter October 2014*

http://www.internetsociety.org/doc/eu-issues-overview-%E2%80%93-18-24-october-2014 , accessed 12.05.2015

EurActiv.com (May 2015) *Member states see digital security as a national issue* http://www.euractiv.com/sections/infosociety/member-states-see-digital-security-national-issue-314967 , Accessed 13.06.2015

European Commission (2013a) – *Commission Staff Working Document – Impact Assessment, accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union*, Strasbourg, 2013*

European Commission (2013b) *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure high common level of network and information security across the Union*, Brussels (2013/0027)*

European Commission (2013c) *EU Cyber Security Strategy – open, safe and secure**

* http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security , accessed 17.03.2015

European Parliament (2013) *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts*, Directorate General for Internal Policies Policy http://www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE_NT(2013)507476_EN.pdf , accessed 17.03.2015

Fleming, J. (April 2015) *Cyber security directive held up in face of 'Wild West' Internet* http://www.euractiv.com/sections/infosociety/cyber-security-directive-held-face-wild-west-internet-313431 , accessed 12.05.2015

Fioretti, G. (9 December 2014) *Internet firms push to be left out of EU cybersecurity law*, http://uk.reuters.com/article/2014/12/09/eu-cybersecurity-idUKL6N0TN3AY20141209 accessed 10.03.2014

Greathouse, C.B. (2014) *Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?* In Kremer, J.F. and Müller, B. (eds.), Cyberspace and International Relations Theory, Prospects and Challenges, www.springer.com/.../9783642374807-c2.pdf , accessed 03.03.2015

ENISA (2014) *An evaluation Framework for National Cyber Security Strategies*, www.enissa.europa.eu

Eriksson, J. & Giacomello, G. (2006), *The Information Revolution, Security, and International Relations: (IR) relevant Theory?*, International Political Science Review, vol. 27: 221-244

Hagedorn, F. *The Community Method vs. Intergovernmental method in the European Constitution*, CONVEU 30 Conference Paper, Center for Applied Policy Reserch http://www.swpberlin.org/fileadmin/contents/products/projekt_papiere/warsaw_hagedorn_sicher.pdf, accessed 08/05/2015

Hammond, B. (February 2013) *Cybersecurity Policy Report*, Aspen Publisher, New York, http://search.proquest.com/docview/1314734832?accountid=8144, accessed 17/03/2015

Jorgensen, Pollack & Rosamond (2006) *Handbook of European Union Politics*, Sage Publications

Kuada, J. (2012), *Research Methodology - A Project Guide for University Students*, Frederiksberg, Aalborg University

Kuada, J. (2014), Research Methods course, PowerPoint presentation, International Business Economics Master programme, Aalborg University

Leuffen, D., Malang, T., Worle, S. (2014) *Structure, Capacity or Power? Explaining Salience in EU Decision Making*, Journal of Common Market Studies, Vol 52, No 3, pp 616-631

Lewis, J. (2003) *Institutional Environments and Everyday Decision-Making; Rationalist or Constructivist? Comparative Political Studies*, Vol. 36, No. ½, pp 97-124

Lewis, J. (2005) *The Janus face of Brussels: socialization and everyday decision making in the EU*, International Organization, Vol. 59, No 4, pp 937-971

Lewis, L (2008) *Strategic bargaining, norms and deliberation: modes of action in the Council of the European Union*, in D. Naurin and H. Wallace (eds), Unveiling the Council: Games Governments Play in Brussels. Palgrave Macmillan, pp 165-184

Moravcsik, A. (1992) *Liberalism and International Relations Theory*, Paper 92-6

Moravcsik, A. (1993) *Preferences and Power in the European Community: A Liberal Intergovernmentalist Approach*, Journal of Common Market Studies, Vol. 31, No. 4

Moravcsik, A. (1995) *Liberal Intergovernmentalism and Integration: A Rejoinder*, Journal of Common Market Studies, Vol. 33, No. 4

North, D.C. (1990) *Institutions, Institutional Change and Economic Performance*, Cambridge and New York: Cambridge University Press

Peterson, J & Bomberg, E. (1999) *Decision - making in European Union*, London: MAcmillan Press LTD

Pierson, P. (1996) *The Path to European integration: an historical Institutionalist approach*, Comparative Political Studies, 29 (2)

Pollack, M. A. (2001) *International Relations Theory and European Integration*, Journal of Common Market Studies, Vol. 39, No. 2, p 221-244

Prinsted, H. (2013) *Methods course, PowerPoint presentation*, European Studies Master programme, Aalborg University

Risse, T. & Wiener, A. (1999) *Something rotten' and the social construction of social constructivism: a comment on comments*, Journal of European Public Policy, Vol. 6, No. 5, pp 775-782

Robson, C. (2011) *Real World Research*, 3rd edition, Wiley

Rosamond, B (2000) *Theories of European Integration*, London: Macmillan Press LTD

Saurugger, S. (2013) *Constructivism and public policy approaches in the EU: from ideas to power games*, Journal of European Public Policy, Vol 20, No. 6, pp 888-906

Schimmelfennig, F. (2001) *The Community Trap: Liberal Norms, Rhetorical Action, and the Eastern Enlargement of the European Union*, International Organization, vol. 55, No 1, pp 47-80, downloaded from http://www.jstor.org/stable/3078597

Schimmelfennig, F. (2015) *Liberal intergovernmentalism and the euro area crisis, Journal of European Public Policy*, 22:2, 177-195, DOI: 10.1080/13501763.2014.9 http://dx.doi.org/10.1080/13501763.2014.99402094020, accessed 09/05/2015

Spain Government (2013), *Paper regarding the Network and Information Security Directive* [Informe 8/2013 de la Comision Mixta para la Union Europea]

Thomas, D. (2008) *The Negotiation of EU Foreign Policy: Normative Institutionalism and Alternative Approaches*, UCD Dublin European Institute Working Paper 08-4.

UK' Government, Department for Business, Innovation and Skills (2013) *Call for Evidence on Proposed EU Directive on Network And Information Security* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/237069/bis-13-1169-call-for-evidence-on-proposed-eu-directive-on-network-and-information-security.pdf , accessed 29.04.2015

UK' Government, Department for Business, Innovation and Skills (2013) *Network and Information Security Directive - Impact Assessment*, https://www.gov.uk/government/uploads/attachment_data/file/244978/bis-13-1206-network-and-information-security-directive-impact-assessment.pdf, accessed 15.04.2015

UK' Parliament (2015) *Ministerial Correspondence, House of Commons European Scrutiny Committee* http://www.parliament.uk/documents/commons-committees/european-scrutiny/MinCor%202014-15.pdf , accessed 25.06.2015

UK' Parliament (2015), *Network Information Security across the EU*, March 2015 http://www.publications.parliament.uk/pa/cm201415/cmselect/cmeuleg/219-xxxvi/21908.htm accessed 29.04.2015

White House (2009) *Cyber Space Policy Review*, American Presidency Office Washington https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf accessed 03.02.2015

Wallace, H., Wallace, W. (2000) *Policy-Making in the European Union*, Oxford: Oxford University Press

Warntjen, A. (2012) *Measuring Salience in EU Legislative Politics*, European Union Politics, Vol. 13, No. 1, pp 168-82

World Economic Forum (2013) *Insight Report - Global Risks 2013*, Eighth Edition http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf , accessed 15.02.2015

ANNEXES

Annex 1 – Position of Co-legislators

Annex 2 - Cyber Security within European Union - Country Summaries

Annex 3 - EU' Cyber Security Maturity Dashboard 2015

Annex 4 – DIGITALEUROPE

Annex 1 – *Position of Co-legislators*

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
concerning measures to ensure a high common level of network and information security across the Union
COM (2013) 48 – 2013/0027 (COD)

COMMISSION PROPOSAL *COM (2013) 0027*	**EP AMENDMENTS** *P7_TA- PROV(2014)244, 13.3.2014*	**COUNCIL AMENDMENTS** *10153/14* ***(As submitted to Coreper 07.11.2014)***	**POSSIBLE COMPROMISE SOLUTIONS/EP PROPOSALS/COMMENTS**
2. To that end, this Directive:		2. To that end, this Directive:	
(a) lays down obligations for all Member States concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems;		(a) lays down obligations for all Member States concerning the prevention, the handling of and the response to **serious** risks and incidents affecting networks and information systems;	The term "serious" is under discussion with the EP
(b) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems;	(b) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated, ~~and~~ efficient ***and effective*** handling of and response to risks and incidents affecting network and information systems ***with the participation of relevant stakeholders***; (AM 40)	(b) creates a cooperation **group** ~~mechanism~~ between Member States in order to **support and facilitate strategic cooperation and the exchange of information among Member States** ~~ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response~~ to risks and incidents affecting ~~network and information systems~~;	Provision to be aligned with art. 8a(1) after the agreement on the latter article
		ba) creates a CSIRTs ("Computer Security Incident Response Team") network in	Provision to be aligned with art. 8b(1) after the agreement on the latter article

Source: Council of the European Union, 2015:9

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
concerning measures to ensure a high common level of network and information security across the Union
COM (2013) 48 – 2013/0027 (COD)

COMMISSION PROPOSAL *COM (2013) 0027*	**EP AMENDMENTS** *P7_TA- PROV(2014)244, 13.3.2014*	**COUNCIL AMENDMENTS** *10153/14* ***(As submitted to Coreper 07.11.2014)***	**POSSIBLE COMPROMISE SOLUTIONS/EP PROPOSALS/COMMENTS**
the operation of networks and information systems, in the event of a risk or an incident affecting them;			
		(6a) "National NIS strategy" means a framework providing high-level vision, objectives and priorities on NIS at national level;	Provision to be read in conjunction with art. 6
(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;	(7) 'incident handling' means all procedures supporting the ***detection, prevention***, analysis, containment and response to an incident; (AM 50)	(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;	Discussions with the EP on the need to keep the words "detection" and "prevention"
(8) "market operator" means:		(8) ~~"market operator" means:~~	
(a) provider of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II;	***Deleted*** (AM 51)	deleted	deleted

Source: Council of the European Union, 2015:25

Annex B

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning measures to ensure a high common level of network and information security across the Union

COM (2013) 48 – 2013/0027 (COD)

COMMISSION PROPOSAL *COM (2013) 0027*	**EP AMENDMENTS** *P7_TA- PROV(2014)244, 13.3.2014*	**COUNCIL AMENDMENTS** *10153/14* ***(As submitted to Coreper 07.11.2014)***	**POSSIBLE COMPROMISE SOLUTIONS/EP PROPOSALS/COMMENTS**
		~~bodies and the other relevant actors;~~]	bodies and the other relevant actors;
(c) The identification of the general measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors;		(c) The identification of the general measures on preparedness, response and recovery [, including cooperation mechanisms between the public and private sectors];	(c) The identification of the general measures on preparedness, response and recovery, including ~~cooperation mechanisms between~~ ***those taken jointly by*** the public and private sectors;
(d) An indication of the education, awareness raising and training programmes;		(d) An indication of the education, awareness raising and training programmes **relating to the NIS strategy**;	(d) An indication of the education, awareness raising and training programmes ***relating to the NIS strategy***;
(e) Research and development plans and a description of how these plans reflect the identified priorities.		~~(e) Research and development plans and a description of how these plans reflect the identified priorities.~~	(e) ***An indication of the research*** ~~Research~~ and development plans ***relating to the NIS strategy*** ~~and a description of how these plans reflect the identified priorities;~~

Source: Council of the European Union, 2015:33

Annex 2 - *Cyber Security within European Union - Country Summaries*

Source: BSA The software Allince (2015) EU Cybersecurity Dashboard - A Path to a Secure European Cyberspace, pp 11-16

Austria

The Austrian government adopted in 2013 a National Cyber Security Strategy, part of a large ICT security initiative. The Strategy, a comprehensive plan, establishes cyber security objectives in various fields of action. Additionally. Austria has established a CERT with a broad and well- defined scope. Moreover, several public-private partnerships operate in the country, such as the Centre for Secure Information Technology Austria (A-SIT).

As an initiative of CERT.at and the government, The Austrian Trust Circles was created, platforms that provide formal structures for sector-specific information exchanges related to the critical information infrastructure of various sectors.

Bulgaria

No national cyber security strategy exists and the legal framework is limited. Also, no formalised public- private partnerships exists, however, cyber security events and academic discussions focused on cyber security and critical information infrastructure protection take place in the country.

CERT Bulgaria illustrates the government efforts to strengthen cyber security, being the most significant cybersecurity entity.

Denmark

At this point Denmark does not have a national cyber security strategy; however a law establishing the Centre for Cyber Security was passed in 2013. The Centre for Cyber Security takes control of and supersedes its current government CERT. Additionally the Danish private sector has a formal framework for cooperation on cybersecurity issues within the body of the Council for Digital Security.

Estonia

Estonia was one of the first EU MSs that developed a national strategy, following the cyber attacks from 2007. The 2008 national cyber security strategy was updated in 2014. Besides this, Estonia has a well-established CERT and a developed legal framework that covers information security. Even if there is no official PPP, the public sector works closely with private sector organisations. Further to national bodies, also notable is the fact that NATO’s Cyber Security Centre of Excellence is based in Estonia.

France

Adopted in 2011, France national cybersecurity strategy is focused on defence and national security issues. Dedicated to information security and integrated with the French CERT, the National Agency for the Security of Information Systems (ANSSI) has taken a targeted approach in managing cyber security by published sector-specific security measures.

Germany

In 2011 was published Germany national cybersecurity strategy, a comprehensive document that is complemented by a strong cybersecurity legal framework. Besides a Federal Office for Information Security (BSI), which is in charge of managing computer and communication security at German government level, Germany also has a network of CERTs, working in collaboration with both state-level and non-governmental CERTs.

Additionally, Germany national policies and legal framework focus on the public- private partnership; examples in this case are Alliance for Cyber- Security and the UP KRITIS partnership.

Greece

Greece has a limited legal and institutional framework within cybersecurity, without a national strategy in place. There is no public-private partnership structure and the national CERT is limited to government institutions and public operators of critical infrastructure.

Ireland

Limited national legal and policy framework in the field of cybersecurity. A national strategy is being developed, and Ireland is in the process of establishing a national CERT. In addition to the private sector entities that are active in the field, there are also some public funded education campaigns, for example "Male IT Secure" that include, besides, online information, a television advertising campaign.

Romania

In Romania a vague cybersecurity strategy was adopted in 2013, currently the legal framework is limited. Some legislative proposals have been submitted to the parliament for adoption, however few were declared unconstitutional as it was pushing the boundary of privacy. The current strategy envisage the establishment of another two agencies in the field of network information and cyber security, besides the national CERT that covers all users of Romanian network.

Spain

As shown in the EU Cybersecurity Dashboard (2015) Spain has adopted a National Cyber Security Strategy in 2013. The Strategy, a comprehensive document in line with existing national security laws and the National Security Plan, sets objectives and lines of action that work together as a package.

Within the framework of the National Strategy, the main agency for information security and cyber security was established, the National Centre for Critical Infrastructure (CNPIC). The Nation Centre is working on several plans: ensuring coordination and cooperation between the public and private sector; runs working groups within specific sectors; working towards the development of sector specific cyber security plans. Additionally, Spain has established two CERTs, namely INTECO-CERT and CCN-CERT with the role of dealing with cyber security incidents.

In terms of cooperation with the private sector, this is formalised through the National Advisory Council on Cybersecurity, a working group established in 2009 with representatives from the private sector. The main task of the Council is policy advice to the government. Moreover, at central level, in matters of policy and lobbing, private sector associations are active in the cyber security and information security sector, and also in general IT matters. (BSA The Software Alliance, 215)

In regards with the NIS Directive, Spain has shown its support for the Directive, although several points need to be changed. One is the mandatory measure of reporting cyber-attacks.

United Kingdom

A comprehensive cybersecurity strategy was published in 2011. Moreover, UK has a strong cybersecurity legal framework and two CERTs: one that supports operators of critical infrastructure and one with focus one the government agencies. The National Security Council and the Office of Cyber Security and Information Assurance are two other relevant bodies in the field of cyber security in UK.

Additionally, a well-developed system of public-private partnerships in which the private sector actively participates on a voluntary basis was established. An example is the Centre for the Protection of National Infrastructure (CPNI) that organises sector-specific information exchanges and covers 14 sectors.

Annex 3 - *EU' Cyber Security Maturity Dashboard 2015*

- **Following on the next page**

Source: BSA The software Allince (2015) EU Cybersecurity Dashboard - A Path to a Secure European Cyberspace, pp 8-9

✔ Yes ✖ No ◑ Partial

#	QUESTION	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France	Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
	LEGAL FOUNDATIONS																												
1.	Is there a national cybersecurity strategy in place?	✔	✔	✖	✖	✔	✔	✖	✔	✔	✔	✔	✖	✔	✖	✔	✔	✔	✔	✖	✔	✔	Draft	✔	✔	✖	✔	✖	✔
2.	What year was the national cybersecurity strategy adopted?	2013	2012	–	–	2013	2011	–	2014	2013	2011	2011	–	2013	–	2014	2014	2011	2013	–	2013	2013	–	2013	2008	–	2013	–	2011
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	◑	◑	✖	✖	✔	✖	✔	✔	✖	✔	✔	◑	✖	✔	✖	◑	✖	◑	✔	✔	✖	✔	✔	✔	✔	✔	✔
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	✖	✖	✖	✖	✔	◑	✔	◑	✖	✖	◑	✔	✖	✖	✖	✖	✖	◑	◑	✖	✖	✖	◑	✖	✖	✔	◑
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✖	✔	✖	✔	✔	✔	✖	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✔	✖	✖	✖	✖	◑	✖	✔	✔	✖	Draft	✖	✖	✖	✖	✔	◑	◑	◑	◑	✖	◑	✖	✖	◑	◑	✖	✖
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	✖	✖	◑	✖	✔	✖	✔	✔	✖	Draft	✖	✔	✖	✔	✖	◑	✖	✖	✔	✖	◑	✖	◑	✖	✖	✖	◑
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	◑	✖	✖	✔	✔	✖	✔	✖	✖	✔	✖	✖	✖	✖	✔	✔	✖	✔	✖	✔	✖	◑	✖	✔	✖	✖	✖
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	✔	✔	✖	✖	✔	✔	✔	✔	✖	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	◑	N/A	N/A	N/A	◑	✔	✔	✔	◑	✔	✔	✔	N/A	✔	◑	◑	◑	N/A	✔	◑	N/A	◑	✖	N/A	✔	✔	◑
	OPERATIONAL ENTITIES																												
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
2.	What year was the computer emergency response team (CERT) established?	2008	2008	2008	2009	–	2011	2009	2008	2014	2008	2012	2009	2013	–	2014	2006	2006	2011	2002	2012	2008	2008	2011	2009	2010	2008	2003	2014
3.	Is there a national competent authority for network and information security (NIS)?	◑	✔	✔	✔	◑	✔	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	◑	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
5.	Are national cybersecurity exercises conducted?	✔	✔	✔	◑	◑	◑	✔	✔	✔	✔	✔	✔	◑	✔	✔	✔	◑	◑	◑	✔	◑	◑	◑	✔	◑	◑	✔	✔
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	✖	◑	✖	✖	✔	◑	◑	✖	✖	✖	✖	✔	✖	✔	✔	◑	◑	✖	✔	✔	◑	◑	✖	✖	✔	◑	✔
	PUBLIC PRIVATE PARTNERSHIPS																												
1.	Is there a defined public private partnership (PPP) for cybersecurity?	✔	◑	◑	◑	◑	✖	✖	◑	◑	✖	✔	✖	◑	✖	◑	✖	✖	✖	◑	✔	✖	◑	✖	✖	✖	✔	◑	✔
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	✔	◑	✖	✖	✖	✔	◑	✔	✖	✔	✖	◑	✔	◑	✖	◑	✖	✖	✔	◑	✖	◑	◑	◑	✔	◑	✔
3.	Are new public private partnerships in planning or underway (if so, which focus area)?	✔	–	✖	✖	✖	◑	✖	✖	✖	◑	✔	✖	✖	✖	◑	◑	◑	◑	✖	–	✖	✖	✔	✖	✖	–	✖	–
	SECTOR SPECIFIC CYBERSECURITY PLANS																												
1.	Is there a joint public private sector plan that addresses cybersecurity?	✔	✖	✖	◑	◑	✖	✖	✖	◑	✔	✖	✖	◑	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✔	✖	✔
2.	Have sector specific security priorities been defined?	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	◑	✖	◑
3.	Have any sector cybersecurity risk assessments been conducted?	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
	EDUCATION																												
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	◑	◑	✖	✖	✔	✖	✔	✔	✔	◑	✖	✔	◑	✔	✔	✔	✔	✖	✔	✔	✖	✔	✔	✖	✔	✖	✔

Annex 4 – *DIGITALEUROPE*

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 57 global corporations and 33 national trade associations from across Europe. In total, 10,000 companies employing two million citizens and generating €1 trillion in revenues. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

THE MEMBERSHIP OF DIGITALEUROPE

COMPANY MEMBERS:

Acer, Alcatel-Lucent, AMD, APC by Schneider Electric, Apple, Bang & Olufsen, BenQ Europa BV, Bose, Brother, Canon, Cassidian, Cisco, Dell, Epson, Ericsson, Fujitsu, Hitachi, HP, Huawei, IBM, Ingram Micro, Intel, JVC Kenwood Group, Kyora Document Solutions, Kodak, Konica Minolta, Kyocera Mita, Lexmark, LG, Loewe, Microsoft, Mitsubishi Electric, Motorola Mobility, Motorola Solutions, NEC, Nokia, Nokia Siemens Networks, Océ, Oki, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion, Ricoh International, Samsung, SAP, Sharp, Siemens, Sony, Swatch Group, Technicolor, TP Vision Texas Instruments, Toshiba, Xerox, ZTE Corporation.

NATIONAL TRADE ASSOCIATIONS:

Belgium: AGORIA; **Bulgaria:** BAIT; **Cyprus:** CITEA; **Denmark:** DI ITEK, IT-BRANCHEN; **Estonia:** ITL; **Finland:** FFTI; **France:** SIMAVELEC; **Germany:** BITKOM, ZVEI; **Greece:** SEPE; **Hungary:** IVSZ; **Ireland:** ICT IRELAND; **Italy**: ANITEC; **Lithuania**: INFOBALT; **Netherlands:** ICT OFFICE, FIAR; **Poland:** KIGEIT, PIIT; **Portugal:** AGEFE; **Romania:** APDETIC; **Slovakia:** ITAS; **Slovenia:** GZS; **Spain:** AMETIC, **Sweden:** IT&Telekomföretagen; **United Kingdom:** INTELLECT
Belarus: INFOPARK; **Norway:** IKT NORGE; **Switzerland:** SWICO; **Turkey:** ECID, TESID, TÜBISAD; **Ukraine:** IT UKRAINE.

Source: DIGITALEUROPE 2013:5