



Institut d'études européennes
Université catholique de Louvain



Institut d'études européennes
Université Saint-Louis - Bruxelles

The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity

Dissertation submitted by **Louis BRUN**
Master 120 of European Studies
Academic year 2017-2018

Supervisor: Dr. Rocco BELLANOVA
Second Reader: Dr. Alexandre DE STREEL

‘I declare on my honour that this dissertation is my own work, completed without unauthorised external assistance, that it has been submitted to no another institution for assessment, and that it has never been published, either in whole or in part. All the information (ideas, sentences, graphs, maps, tables, etc.) taken from or referring to primary or secondary sources are properly referenced using the current university method. I declare that I have taken note of and adhere to the Code of Ethics for students with regard to borrowing, quoting from and using various sources, and am aware that plagiarism is a serious offence.’

Table of content

Introduction.	4
Chapter 1: Literature review.	6
1.1 The European Union as a cyber power.	6
1.2 ENISA: the right arm of the European cybersecurity.	8
Chapter 2. Theoretical framework.	10
2.1 ENISA and the principal-agent theory.	10
2.2 A brief explanation on the subject of European regulatory agencies.	10
2.3 Agents, principals and endorsers.	12
2.4 Costs and benefits of delegation.	13
2.5 Autonomy against accountability.	13
2.6 Conclusion: politics of delegation and of discretion.	14
Chapter 3: Research design.	16
3.1 Research question.	16
3.2 Research hypotheses.	17
Chapter 4: ENISA and the European cybersecurity policies.	19
4.1 The European cybersecurity policies: a fragmented landscape.	20
4.1.1 The 2013 European cyber strategy: an approach in three axis.	21
4.1.2 The Network and Information Security policy.	23
4.2 The European Network and Information Security Agency.	26
4.2.1 A legal basis under the article 95 TEC/ 114 TFEU: a controversial choice?	26
4.2.2 The evolution of ENISA's missions and tasks.	28
Chapter 5: ENISA's internal institutions and control mechanisms.	32
5.1 ENISA and the politics of discretion.	32
5.2 The executive director.	33
5.3 The management board	36
5.3.1 Composition, meetings, voting procedures of the management board.	36
5.3.2 The Management board's internal debates.	38
5.4 Financial and budgetary resources.	40
5.5 ENISA's discretion and its control mechanisms.	42
Chapter 6: the legislative debates regarding ENISA's acts of delegation.	45
6.1 The methodological, theoretical and research aspects of this chapter.	45
6.1.1 Theoretical considerations: actor-mapping and principals viewed as a collective.	45
6.1.2 Sources: availability and types.	46

6.2	The 2004 and 2008 regulations.....	47
6.3	The 2011 and 2013 regulations.....	51
6.4	The 2018 regulation.....	55
6.5	The balance of power between the European Parliament and the Council of the European Union in regards of ENISA’s acts of delegation.	57
Conclusion:		59
a.	Findings of the research regarding the first research hypothesis: “ <i>The European Parliament and the Council of the European Union are the two principals of ENISA. The European Parliament tends to advocate for a supranational agenda while the Council of the European Union tends to defend an intergovernmental agenda</i> ”	60
b.	Findings of the research regarding the second research hypothesis: “ <i>The management board of ENISA is the main control mechanism set by the principals and defends intergovernmental interests</i> ”	61
Bibliography		62
1)	Collective works:.....	62
2)	Monographs:.....	62
3)	Academic article:.....	62
4)	Official publications:	63
a)	European Commission	63
b)	Council of the European Union.....	64
c)	European Parliament.	65
d)	ENISA.	65
e)	European Court of Justice, Europol and the Official Journal of the European Union.	66
5)	Internet sources:	66

Introduction.

In its 2017 speech on the state of the Union¹, the President of the Commission Jean-Claude Juncker presented one of the most pressing issues regarding the new industrial policy of the Union: the digitalization of the European economy and society². This process is now considered as an established economic trend and the European officials have qualified it as the most recent industrial revolution transforming the dynamics and solidarities influencing every aspects of the European future.

Indeed, the digitalization of the European economy has created new challenges and opportunities which must be addressed by the European institutions and the governments of its Member States. From the threat of cyber criminality, the protection of critical infrastructures to the confidence of the European consumers in the growing digital market, the European institutions were quick to provide answers in order to cope with these new questions.

The 2016 cyber package is the most recent incarnation of these solutions³. The goal of this policy package is the reinforcement of policies aiming at insuring the security and prosperity of a single market increasingly influenced by the introduction of new products and services issued from the development of Information and Communication Technologies (ICT). The cyber package touched many aspects of the European governance, regarding the digital economy, but increased tremendously the role of a specific agency: the European Network and Information Security Agency (ENISA).

ENISA is not a recent actor in the European governance as it was founded in 2004. However, the agency has seen its role in the European cybersecurity policies becoming more and more important with each year passing. Once considered as an advisory body of the European governance, the agency is now gaining operational tasks influencing key aspects of national cybersecurity policies.

This evolution, from advisor to operational actor, wasn't a linear process and the evolution of ENISA was riddled with challenges and conflicts. The main reason of these confrontations on ENISA's future was due to a single fact at the core of ENISA's mandate: what the European institutions called harmonization of the single digital market, the Member States considered it as being matters of national security. Indeed, ENISA's governance influences policies such as the protection of critical infrastructures throughout the Union as well as the establishment of common certifications regarding ICT goods and services. Henceforth, it can be argued that ENISA's mandate has both an economic aspect and a security dimension. This opposition will be more thoroughly discussed in the next chapters.

This contradiction has determined every aspect of the debates on ENISA's future at the European level. Five regulations have been or will be introduced on ENISA and each of these regulations defines legally the agency's mandate. Conclusively, this dissertation will

¹ European Commission, *PRESIDENT JEAN-CLAUDE JUNCKER'S State of the Union Address 2017*, Brussels, 2017, SPEECH/17/3165.

² European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT? THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, THE COMMITTEE OF REGIONS AND THE EUROPEAN INVESTMENT BANK: Investing in a Smart, Innovative, and Sustainable Industry, a Renewed EU Industrial Policy Strategy*, Brussels, 2017, COM(2017) 479 final.

³ European Commission, Digital Single Market: Policies: Cybersecurity, <https://ec.europa.eu/digital-single-market/en/cyber-security>, consulted on the 02/08/2018.

understand how these tensions between national safety and the necessary harmonization of booming sectors of the European economy have influenced the institutionalization of the agency.

The subject of this dissertation is *“the role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity”*. The importance of the conflicting national and European interests in the development of ENISA invites us to consider the following research question: *“How does intergovernmental and supranational interests have influenced the institutionalization of ENISA?”*.

As such, the opposition of intergovernmental and supranational interests will be the guiding theme of this dissertation. This theme will be studied by the analysis of debates both internal and external to the agency. The objective will be to determine how this conflict has influenced the institutionalization of ENISA internally, within the agency’s internal institutions, and externally, during the interinstitutional negotiations between the European institutions on the different regulations determining ENISA’s mandate.

In this regard, two research hypotheses will be formulated. The first will consider the interinstitutional debates and will be formulated as following: *“The European Parliament and the Council of the European Union are the two principals of ENISA. The European Parliament tends to advocate for a supranational agenda while the Council of the European Union tends to defend an intergovernmental agenda”*. The second hypothesis will be focused on the internal functioning of ENISA and will be formulated as following: *“The management board of ENISA is the main control mechanism set by the principals and defends intergovernmental interests”*. The different aspects of these hypotheses will be detailed in the third chapter of this dissertation: the research design.

In order to address properly the research question, this dissertation will be divided in six different chapters. The first chapter will be the literature review and will present the state of the scientific literature on the subject of ENISA’s actions and the development of the European cybersecurity policies. The second chapter will be the theoretical framework presenting the theoretical assumptions on which this dissertation analysis are based: the principal agent-theory. The third chapter is the research design and will develop the research question and the research hypotheses while discussing the methodological aspects of the analysis and the sources used in this dissertation. These three first chapters are to be understood as the formal introduction of the dissertation. The fourth chapter will present the European cybersecurity landscape and the particular role of ENISA within these policies. The fifth chapter will detail ENISA’s internal institutions and the control mechanisms set by the European institutions to control the agency’s governance. This fifth chapter will discuss the second research hypothesis. The sixth chapter will describe the interinstitutional negotiations on the different regulations founding ENISA’s mandate and will discuss the first hypothesis.

Chapter 1: Literature review.

As the European cybersecurity is a relatively recent field of study, the scientific literature surrounding this subject is quite heteroclitic and, yet, surprisingly rich. Many of these authors have a very factual approach of the European cybersecurity, however some of them have produced some extensive and specialized works developing an analysis on almost all of the dimensions of the European cybersecurity⁴.

In order to present the main themes commonly addressed in the scientific literature, we will divide the literature review into two distinct parts. Firstly, we will present the European Union's role in the European cybersecurity and the authors' perceptions of the particularities of the Union as a cyber power. Secondly, we will address more specifically the position of ENISA in the literature and the critics that may have occurred against this agency.

1.1 The European Union as a cyber power.

The analysis of the authors on the EU, as a cyber power, does not focus heavily on the fundamental elements of the EU cybersecurity. For example, the organization of the EU in three pillars (defense, cyber criminality and Network and Information Security) as well as the multilevel approach of the European cybersecurity (European level, national level and private level) are looked upon as an almost natural method of organization⁵. The post-2013 literature does not present any alternative to the current institutional model. Nevertheless, Authors, such as Christou⁶, have been more openly critical of the European approach of cybersecurity than the others.

A first theme vividly discussed by the intellectual community is the nature of the EU not only as cyber power but also as security provider. Sliwinski⁷ provides here an interesting insight on how the EU has to act in order to establish a pertinent model of cybersecurity.

Sliwinski⁸ observes that the EU suffers from a certain number of limitations influencing its capacity to behave as a cyber power. The first of these limitations is the apparent heterogeneity amongst the Member States regarding the national models of cybersecurity policies and institutions. In other words, as the operationalization of cybersecurity is a national responsibility, each Member State has produced different models of national cybersecurity institutions and strategies. This point has been observed by numerous authors in different fashions⁹. For Sliwinski¹⁰, the intergovernmental nature of the Common Foreign and Security Policy (CFSP) and Common Security and Defense Policy (CSDP), along with the rapid

⁴ CHRISTOU, George, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Hampshire, Palgrave Macmillan, 2016.

⁵ LEISTERER, Hannfried, New EU cyber security legislation: a Q & A with Andreas Schwab, internet policy review-journal on internet regulation, <https://policyreview.info/articles/news/new-eu-cyber-security-legislation-q-andreas-schwab/411>, consulted on 14/07/2017.

⁶ CHRISTOU, George, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Hampshire, Palgrave Macmillan, 2016, p.171-189.

⁷ SLIWINSKI, Krzysztof Feliks, "Moving beyond the European Union's Weakness as a Cybersecurity Agent", *Contemporary Security Policy*, 35:3, 2014, p.472-474.

⁸ SLIWINSKI, Krzysztof Feliks, "Moving beyond the European Union's Weakness as a Cybersecurity Agent", *Contemporary Security Policy*, 35:3, 2014.

⁹ BARRINHA, André, CARRAPICO, Helena, "The EU as a Coherent (Cyber) Security Actor?", *Journal of Common Market Studies*, JCMS 2017, UACES, 2017, p.2-6.

¹⁰ SLIWINSKI, Krzysztof Feliks, "Moving beyond the European Union's Weakness as a Cybersecurity Agent", *Contemporary Security Policy*, 35:3, 2014, p.479-482.

institutionalization of the European Cybersecurity, is an obstacle for the standardization of the national cybersecurity institutions.

The lack of cohesion and common vision amongst the Member States is the most prominent concern expressed by the scientific community. Carrapico and Barrinha, in their common article, have expressed concerns on the lack of coherence of the European cybersecurity landscape as Member States belonging to the Visegrad Group, with the addition of Austria, form their own cybersecurity organization under the name of CSCSP¹¹.

Another substantial limitation, noticed by Sliwinski¹², is the civilian nature of the EU that delegitimized its role as a security provider. The comparison with NATO is here unavoidable by many of the authors¹³. Lewinski notices that NATO may be seen as a more legitimate actor regarding cybersecurity due to its nature. The defensive nature of the EU established a *de facto* limitation on the subject of cyber defense relegating the European cybersecurity to its more natural role like Network and Information Security or the suppression of cyber criminality.

In this regard, the civilian nature of the EU also developed two of the main particularities of the European model: the multilateralism and the “stakeholderism¹⁴”. These two notions are quite widespread in the literature as well¹⁵. These two concepts serve the pragmatic purpose of improving the European cyber resilience but also highlight the more implicit goal of the EU knowingly to insure the spreading and diffusion of European standards of cybersecurity¹⁶. Along with these two notions, authors like Myriam Dunn Cavelty¹⁷ have also pointed out the importance of the debate on the place of the core values of the EU in the European cybersecurity.

Ultimately, the importance of “stakeholderism”, European core values and multilateralism is being viewed as a testimony of the nature of the EU as a cybersecurity agent and how the European institutions plan to overcome the limitations induced by the nature of the Union itself. The Union intends to rely on its soft power created by the diffusion of European norm as well as its capacity to encourage socialization of the different actors, private as public, involved in the European cybersecurity¹⁸. Christou¹⁹ and Sliwinski²⁰ are the authors that most explicitly present the importance of soft power in the European cybersecurity. In this regard, Sliwinski sees the over-institutionalization of the European cybersecurity, at the European level, as a way

¹¹ BARRINHA, André, CARRAPICO, Helena, “The EU as a Coherent (Cyber) Security Actor?”, *Journal of Common Market Studies*, JCMS 2017, UACES, 2017, p.11-12.

¹² SLIWINSKI, Krzysztof Feliks, “Moving beyond the European Union's Weakness as a Cybersecurity Agent”, *Contemporary Security Policy*, 35:3, 2014, p.476-478.

¹³ RENARD, Thomas, “The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security”, *European Strategic partnership observatory*, working paper 7-June 2014, 2014, p.16-20.

¹⁴ CHRISTOU, George, “The EU's Approach to Cyber Security”, *EUSC EU-China Security Cooperation: performance and prospects*, Policy paper series, Autumn/Winter 2014, 2014, pp.5.

¹⁵ RENARD, Thomas, “The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security”, *European Strategic partnership observatory*, working paper 7-June 2014, 2014.

¹⁶ SLIWINSKI, Krzysztof Feliks, “Moving beyond the European Union's Weakness as a Cybersecurity Agent”, *Contemporary Security Policy*, 35:3, 2014, p.472-474.

¹⁷ DUNN CAVELTY, Myriam, “A RESILIENT EUROPE FOR AN OPEN, SAFE AND SECURE CYBERSPACE”, *Swedish Institute of International Affairs*, number 25 December 2013, 2013, p.4-5.

¹⁸ BACKMAN, Sarah, “Organizing National Cybersecurity Centers”, *Information & Security: An International Journal*, volume 32-2015, 2015, p.5-12.

¹⁹ CHRISTOU, George, “The EU's Approach to Cyber Security”, *EUSC EU-China Security Cooperation: performance and prospects*, Policy paper series, Autumn/Winter 2014, 2014, p.6-10.

²⁰ SLIWINSKI, Krzysztof Feliks, “Moving beyond the European Union's Weakness as a Cybersecurity Agent”, *Contemporary Security Policy*, 35:3, 2014, p.476-479.

to force the Member States to adopt national cybersecurity policies at a pace agreeable to the European political agenda in regard of the development of efficient European cybersecurity policies.

Furthermore, most of the authors complain of the lack of conceptual framework to analyze the cybersecurity issues especially in a complex European context. The lack of conceptual clarity is one of the main issues on this matter and will be examined further in the part dedicated to the place of ENISA in the scientific literature.

1.2 ENISA: the right arm of the European cybersecurity.

The purpose of ENISA mirrors the role of the EU, as a cyber power, in much of the literature. ENISA is being seen as a facilitator, a regulator and an agent of socialization corresponding to the need of the “soft” approach of the EU regarding the harmonization of the national cybersecurity policies. In many ways for the scientific community, ENISA is a direct response to the apparent lack of legitimacy of the Union as a cyber power and the heterogeneity of the Member States in regard of cybersecurity practices and policies. Moreover, regarding ENISA, the literature understands the cybersecurity as the capacity to insure the readiness of the national and European institutions and actors to face major cybersecurity incidents. Thus, ENISA plays a role in the preparation of cybersecurity agents by diffusing information and good practices regarding cybersecurity²¹.

Obviously, the authors have noticed the separation in three pillars of the European cybersecurity and have confined ENISA in the Network and Information Security (NIS) part of this organizational layout. Nevertheless, most authors didn't present the many dimensions of the Network and Information Security pillar of the European cybersecurity strategy. Only certain authors tackle explicitly this issue such as Carrapico and Barrinha²². Evidently, ENISA in itself is not being viewed as a subject of study for the intellectual community but is strongly associated with the EU as a cyber agent.

The action of ENISA is satisfying for the majority of the authors. Despite the multiplication of the actors in the European cybersecurity landscape since 2013, the role of ENISA has been presented as being unambiguous and clearly separated from the other agencies such as the European Defense Agency (EDA) or the European Cybercrime Center (EC3). ENISA pursues the objectives of the EU concerning the development of cybersecurity approach based on stakeholderism and multilateralism. In this regard, the role of ENISA as an agent of diffusion of the European standards and values is perfectly understood by the authors. Nevertheless, some among the intellectual community are more critical than others regarding the action of ENISA.

The demonstration of explicit oppositions toward the action of ENISA is rare and undeveloped from an intellectual perspective. For example, in their works²³, Herrington and Aldrich describe

²¹ CHRISTOU, George, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Hampshire, Palgrave Macmillan, 2016, pp.2.

²² BARRINHA, André, CARRAPICO, Helena, “The EU as a Coherent (Cyber) Security Actor?”, *Journal of Common Market Studies*, JCMS 2017, UACES, 2017, p.2-6.

²³ ALDRICH, Richard, HERRINGTON, Lewis, “The Future of Cyber-Resilience in an Age of Global Complexity”, *Political Studies Association*, 2013- vol.33 (4), 2013.

ENISA as a paper tiger, an agency without true operational capacities which produces no other effects than the complexification of national cybersecurity institutions and strategies.

However, other authors have criticized ENISA in a more constructive manner. One of the most common critics is the obsolescence of some of the missions of ENISA, such as the creation of a common European culture of cybersecurity. Nevertheless, these critics have to be contextualized as the development of a common cybersecurity culture is being seen as an objective of the 2004 regulation²⁴ that has to be surpassed by the 2016 NIS directive²⁵ in order to promote a better European integration of cybersecurity.

This critic on the outdated approach of the emergence of a European cybersecurity culture is mainly supported by Carrapico, Barrinha, Lewinski or again Bosco²⁶. On this matter, Karine e Silva²⁷ formulates the most developed commentaries. Apparently, if ENISA is the designated institution to solve the lasting issue of conceptual clarity, the lack of precision on NIS related topics proposed by ENISA is being counterproductive to the establishment of a European cybersecurity culture. Moreover, the problem of the lack of conceptual clarity partially explains the reluctance of the Member States to follow the European recommendations concerning cybersecurity.

This issue of conceptual clarity is a lingering theme among the authors but seems to designate a certain number of realities. On the one hand, authors such as Christou describe this issue as being a handicap for the scientific community²⁸. On the other hand, other authors, such as Lewinski and e Silva, see the issue of this lack of true definitions as an institutional problem creating obstacles among Member States on the national and international level alike.

Ultimately, this situation, where the lack of conceptual clarity exists on both the intellectual and the institutional level, represents quite well the role of ENISA. The agency role as a hub of experts is being felt and noticed by public and private actors. Interestingly, the importance of ENISA as a theorist is being challenged by several institutions such as NATO²⁹ and the European Military Staff³⁰. Even though this last statement is never explicitly explained by the authors, it is understandable as ENISA evolves in a dynamic environment where actors are getting more and more concerned by the evolution of cybersecurity.

²⁴ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1.

²⁵ European Commission, *Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, Brussels, 2016, L 194/1.

²⁶ BOSCO, Francesca, *Assessing Europe's Cyber challenges*, internet policy review-journal on internet regulation, <https://policyreview.info/articles/news/assessing-europes-cyber-challenges/355>, consulted on 14/07/2017.

²⁷ E SILVA, Karine, « Europe's fragmented approach towards cybersecurity », *INTERNET POLICY REVIEW Journal on internet regulation*, volume 2 issue 4, 2013, p.2-4.

²⁸ CHRISTOU, George, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Hampshire, Palgrave Macmillan, 2016, p.11-33.

²⁹ SLIWINSKI, Krzysztof Feliks, "Moving beyond the European Union's Weakness as a Cybersecurity Agent", *Contemporary Security Policy*, 35:3, 2014, p.474-475.

³⁰ European Security and Defense College, *Handbook CSDP: the Common Security and Defense Policy of the European Union*, Vienna, 2016, volume I 3st edition, p.121.

Chapter 2. Theoretical framework.

The literature review has shown that the studies of the academic community regarding the evolution of the European cybersecurity policies revolved around a few selected themes. The question of institutionalization, of states heterogeneity and of European governance through the use and development of agencies are recurring themes and all highlight the importance of interactions among numerous actors.

This chapter will present the theoretical framework which we will be using in the analysis of the actions of ENISA in regard of the institutionalization of the European cybersecurity policies. In this dissertation, the theoretical framework will be based upon the principal-agent theory. This theory will allow us to study and understand the relationships between the different national and European actors in the evolution of ENISA.

2.1 ENISA and the principal-agent theory.

ENISA is one of the milestone of the development of the European cyber policies toward an efficient cybersecurity. Since 2004³¹, ENISA is the focal point of every aspects of the European NIS policy. By advising and designing guidelines for all kind of actors, ENISA is at the crossroad of the build-up of cyber defense, cyber resilience and the struggle against cyber criminality. Furthermore, ENISA acts on matters closely related to Member States' security while insuring the homogenization of a fragmented European digital market.

The centrality of ENISA in the European cybersecurity landscape makes it influential for both European and national interests. In the debates around the development of the European cybersecurity policies, every institutional actors defend their interests depending on their supranational or national leanings. Henceforth, the principal-agent theory will allow us to understand the positions of every actors and how these positions have influenced the institutionalization of ENISA.

As such, the importance of the principal-agent theory is widely recognized by the intellectual community studying matters related to the European agencies³². Synthetically, the principal-agent theory analyses the relation of subordination between the European agencies, as agents, and the European institutions, as principals. This theory emphasizes the importance of the notion of discretion which determines the degree of autonomy of these agencies.

2.2 A brief explanation on the subject of European regulatory agencies.

Before introducing the principal theoretical concepts of the principal-agent theory, it is important to explain in which institutional context this theory evolves. European regulatory agencies respond to the institutional need for a pan European harmonization in sectors where the Union's capabilities were poorly affirmed and where the member States still hold comprehensive competences such as in social, economic or security policies³³.

³¹ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, No 460/2004.

³² JEPPESEN, Lene, TRANDAL, Jarle, "Images of Agency Governance in the European Union", *West European Politics*, 31:3, 2008, p.418-436.

³³ RITTBERGER, Berthold, WONKA, Arndt, "Introduction: agency governance in the European Union", *Journal of European Public Policy*, 18:6, 2011, pp.481.

The researcher Daniel Kelemen has developed the following definition for the European agencies:” *EU level public authorities with a legal personality and a certain degree of organizational and financial autonomy that are created by acts of secondary legislation in order to perform clearly specified tasks*³⁴”. Furthermore, the European agencies all share a similar organizational structure which revolved around an executive director and a management board³⁵.

As such, the competences of the European agencies are relatively limited but crucial in the conduct of the European harmonization. The prominent function of a European agency is to collect data, to produce guidelines and to coordinate private and public actors in order to ease the implementation of national and European policies³⁶.

The creation of a European agency induces political costs for the national and European political leadership. However, the political authorities may enjoy functional and political advantages from the newly created agency. From a functional perspective, an agency allows new governance strategies to the political leadership. As an agency is specifically designed to tackle complex issues on precise technical matters, the professionalism and the technical expertise of the agency is an insurance for the political power that couldn’t otherwise tackle complex policies with the same needed regularity and level of expertise³⁷.

From a political standpoint, the constitution of agencies allows the pursuit of long term political objectives and the definition of a clear agenda. The political credibility of a policy also depends on the ability of the agency to perform as the political leaders intend it to function. Furthermore, agencies contribute to a certain stability of the European institutional system as it offer a compromise between guarantying of Member States ‘sovereignty and the involvement of the European Commission. Politically, the agencies represents a compromise between the national level and the supranational level in order to continue the harmonization without putting too much integration stress on national political system³⁸.

Despite a claimed neutrality, the agencies still hold a certain political power as it guide national policies by their guidelines and advices. The legitimacy of the European agencies, as public actors, revolved around democratic and technocratic justifications. The technocratic legitimacy of an agency relies on its capacity to fulfill its objectives and to respect its mandates while the democratic legitimacy depends on the control mechanism set by the legislator in order to keep agencies under the control of political institutions³⁹.

This notion of legitimacy highlights the main theme of the literature regarding European agencies and the principal-agent theory which is the dialogue between autonomy and accountability of the European agencies.

³⁴ THATCHER, Mark, *The creation of European regulatory agencies and its limits: a comparative analysis of European delegation*, Journal of European Public Policy, 18:6, 2011, pp.796.

³⁵ LORD, Christopher, *The European Parliament and the legitimization of agencification*, Journal of European Public Policy, 18:6, 2001, pp.921.

³⁶ RITTBERGER, Berthold, WONKA, Arndt, ‘EU agencies’ in Richardson, Jeremy, Mazey, Sonia (eds.), *European Union. Power and policy-making*, London, Routledge, 2015, p. 234-237.

³⁷ KELEMEN, Daniel, MAJONE, Giandomenico, ‘Managing Europeanization: the European Agencies’ in Peterson J., Shackleton M. (eds.), *the Institutions of the European Union*. 3rd edition, Oxford, Oxford University Press, 2012, p.225-229.

³⁸ Idem.

³⁹ Ibidem, p.236-237.

2.3 Agents, principals and endorsers.

As we have seen, the European agencies hold a specific role in the European governance. Tackling issues too complex for the classical governance methods, the agencies have to respect requirements of neutrality and professionalism that seems to guarantee their independence. However, the considerable influence of these agencies on the national and European policy-making force the principals to assume the control of these agencies. The principal-agent theory studies this particular relationship between an agents, in this case regulatory agencies, and its principals.

The principal-agent theory belongs to the neo-institutionalism. As such, it follows the principles defined by this school of thought. Specifically, the neo-institutionalist conception of the actors' behaviors is here paramount. Actors act rationally and are self-interested. They seek to maximize their gains in order to serve their interests⁴⁰.

A direct translation of this principle is that if the principals define the structures and objectives of their agents, the principals' final decision on the agent's institutional model and functioning is not only based on the potential efficiency of the agents but also on the political consensus found among the political entities forming the principals concerning the foundation of the new agent. In other words, the agent's structure may be inefficient or inadequate because of the political preferences of the actors constituting the principals⁴¹.

If the identity of the agent is relatively simple to define, as it is the direct subordinate of the principals on the basis of a formal act of delegation⁴² created by the principals, the nature of the principals is more difficult to perceive. The principal is not necessarily a unified entity but can correspond to a group of institutions as well as a single actor. In this regard, a principal constituted by a multitude of different actors is regarded as a collective principal.

As such, the mapping of the principal-agent relations is one of the challenge of the principal-agent theory as it must take into account the interests of potentially several different principals. However, the principal-agent relationships are always hierarchical and bilateral with the principal having authority over the agent even though the agent might have some discretion and powers in this relationship⁴³.

The principal-agent relationship established itself on several levels defined as a chain of delegation. Accordingly, the immediate principal of one agent might be itself the agent of another higher principal. Additionally, a third category of actors called endorser might intervenes in principal-agent relationship. The endorser may seek to influence in the actions of the principal and of the agent by legitimizing the policies of the principal or by vetoing the actions of the agent.

⁴⁰ HALL Peter, TAYLOR Rosemary, "Political Science and the Three Institutionalisms", *Political Studies*, 44(4), 1996, p.942-945.

⁴¹ POLLACK, Mark, "Delegation, agency, and agenda setting in the European Community", *International Organization*, 51(1), 1997, p.106-109.

⁴² ADRIAENSEN, Johan, DELREUX, Tom, "Introduction. Use and Limitations of the Principal-Agent Model in Studying the European Union", in ADRIAENSEN, Johan, DELREUX, Tom (Dir.), *the Principal Agent Model and the European Union*, Basingstoke, Palgrave Macmillan, 2017, p. 3-6.

⁴³ Ibidem, p.12-22.

2.4 Costs and benefits of delegation.

As we have seen, the principals expect functional and political benefits from delegating to an agents. However, the actors in the principal-agent theory are rational and obey to cost-benefit logic. The act of delegation comes with several costs which may refrain the principals to create a new agent.

More prosaically, with the creation of an agent, the principals expects to take advantage of several practical benefits induced by the delegation. The agent represents the chance to set a credible agenda and to take initiatives in order to produce concrete reforms. Furthermore, the careful governance of an agent will also serve to monitor the implementation of new norms while solving the technical problems induced by the change due to the reforms. The ultimate goal of an agent is to propose complex and credible regulation to push the harmonization forward⁴⁴.

Nevertheless, the nature of the political sector, in which the agency evolves, is here paramount as Member States will be reluctant to delegate power on heavily politicized matters or where vital national interests are at stake. Furthermore, the newly created agent may developed a mind of its own due to its institutionalized autonomy. The agent will defined its own interests and adopt opportunistic behaviors in order to defend its preferences. In order to pursuit its interests, the agent might deploy strategies in order manipulate the situations at its advantages at the expense of its principal⁴⁵. The potential defiance or heterogeneity of preferences of the agent toward the principal increases the cost of delegation which dictates the political willingness to create an agent.

Accordingly, the potential confidence of the principal toward the agent is the deciding factors in the cost of delegation. In the eyes of the principal, a low politic, technical sector insures a low cost of delegation and will allow the creation of a highly autonomous agent. However, principals may impose monitoring systems and define sanctions against the agent in order to lower the cost of delegation.

2.5 Autonomy against accountability.

The balance between the autonomy and the accountability of an agent is the defining conflict in the relation between the agent and the principal. If an autonomous agent is being viewed as a clear guarantee of technocratic efficiency, the accountability of this agent toward its principal insure low delegation cost and the democratic legitimacy of the agent.

The principals may design a range of control mechanisms which will define the degree of discretion, or autonomy, enjoyed by the agent. These control mechanisms can be put before or after the actions of the agent.

For instance, there is several kind of *ex post* control mechanisms available to the principals. The principals can monitor the actions of the agent by themselves or by other actors, such as the public opinion or another European agent. Diverse sanctions can be also implemented against the agent. However, each mechanisms come with a cost as monitoring an agent can be

⁴⁴POLLACK, Mark, "Delegation, agency, and agenda setting in the European Community", *International Organization*, 51(1), 1997, p.121-128.

⁴⁵ Ibidem, p.108-113.

time consuming or having the agent sanctioned or under the light of the public opinion may hinder its credibility⁴⁶.

On the other hand, *ex ante* control mechanisms are being proposed when the political decision to create an agent is being made. The mandate of the agent defines the scope of the competences delegated by the principals to the agent as well as the very nature of the agent. The mandate of the agent, therefore, represents the main element of *ex ante* control mechanisms available to the principal⁴⁷.

Ultimately, the potential burden of restrictive control mechanisms represents a psychological threats for the agents and insure that the sheer existence of potential retaliations of the principal against the agent forces the agent to respect its mandate. In other words, the control mechanisms are useful not only because they are being used but because they exist⁴⁸.

It is also important to notice that if the relations between an agent and a principal evolved within the legal framework of a mandate, these interactions, between these two actors, are being made beyond the mechanisms legally set by the mandate and, thus, find a translation within the political world. Accordingly, the agent enjoys a formal autonomy and a practical autonomy, or discretion, while the principals may find other means to control the agent than the control tools defined by the act of delegation⁴⁹.

In conclusion, the dialogue between autonomy and accountability defined the very nature of the agent and is constituted by both legal and practical elements. The autonomy of an agent cannot be defined by abstract levels of discretion but as a continuum of autonomy and accountability defined by the practical and legal interactions of the agent and of the principals. Nevertheless, the importance of informal elements in the Principal-agent relationship highlights the importance of the balance of power between the agent and principals which means that even if the principals are hierarchically superior to the agent, the agent might still gain discretion beyond what is allowed by the act of delegation.

2.6 Conclusion: politics of delegation and of discretion.

The principal-agent theory allows the systematic analysis of the actors involved in a European policies while understanding the different interests motivating these actors. In the case of a study of ENISA, this approach of the study of the European cybersecurity is adequate.

The European cybersecurity policies are being implemented on a fragile equilibrium between the necessities of a Union-wide regulation of the digital market and the imperatives of national security depending on national cybersecurity institutions. In this regard, ENISA is at the center of both European and national interests. Accordingly, we could expect that European institutions might defend different agendas, on the basis of their intergovernmental or supranational leanings, regarding the development of ENISA and of the European cybersecurity policies.

⁴⁶POLLACK, Mark, "Delegation, agency, and agenda setting in the European Community", *International Organization*, 51(1), 1997, p.113-121.

⁴⁷ Idem.

⁴⁸ Idem.

⁴⁹ Idem.

In the literature⁵⁰, it is established that supranational interests are being defended by the European Commission and the European Parliament while intergovernmental interests are being represented by the Council. Such a division within the principals of ENISA, as an agent, could create interesting inconsistency within the mandate of ENISA.

However, this last statement reveals one of the methodological challenges of the principal-agent theory. The regulations, defining the mandate of ENISA, act as an act of delegation designating an agent, ENISA, and a set of principals. But which European institutions can be considered as being an active actor in this set of principals? Where can we separate the principals of ENISA and the endorsers influencing the mandate of ENISA? On the basis of the literature⁵¹, this question can be answered by examining the voting method related to the implementation of the act of delegation or the constitution of the management board of this agency. Henceforth, identifying the set of principals and their interests will be one of the challenges of this dissertation.

This scientific endeavor of understanding which institutions are the principals and what is the interests of these institutions in the institutionalization of the agent is the key aspect of the principal-agent theory's notion of politics of delegation⁵². The politics of delegation aims at explaining the political process that led to the formation of the agent and how the balance of power among the principals during the legislative procedure, resulting in the creation of the act of delegation, influenced the institutionalization of the agent.

Furthermore, the difference between the control, induced by the act of delegation, exercised on ENISA by the principals and the actual discretion of ENISA will be another methodological issue as it forced us to consider the informal aspects of the principal-agent relationship⁵³. The balance between discretion and control is one of the key points of the principal-agent theory as it help to understand the balance of powers between the agent and its principal. In this regard, ENISA offers an interesting case of study as it have had a limited mandate during most of its existence necessitating the approval of its principals while its competences were always progressively being expanding reforms after reforms.

Accordingly, the study of the formal and informal mechanisms of control regulating the discretion of the agent relates to the notion of politics of discretion⁵⁴. The politics of discretion explains the distribution of power among the agent and the principals through the analysis of the diverse mechanisms of control. This distribution of power will then allow the appreciation of the discretion of the agent.

⁵⁰ ANDOURA, Sami, TIMMERMAN, Peter, "Governance of the EU: The Reform Debate on European Agencies Reignited", *European Policy Institutes Network*, working paper n°19/October 2008, 2008, pp.16.

⁵¹ ADRIAENSEN, Johan, DELREUX, Tom, "Introduction. Use and Limitations of the Principal-Agent Model in Studying the European Union", in ADRIAENSEN, Johan, DELREUX, Tom (Dir.), *the Principal Agent Model and the European Union*, Basingstoke, Palgrave Macmillan, 2017, pp. 16.

⁵² Ibidem, p. 18-19.

⁵³ Ibidem, p. 18-22.

⁵⁴ Ibidem, P. 19-22.

Chapter 3: Research design.

As we have seen in the literature review and the theoretical framework, responding to the research question will necessitate to mobilize different conceptual tools in order to analyze the diverse themes regarding the institutionalization of the European landscape. Henceforth in the Research design, we will define the important aspects that will guide the researches on the development of ENISA.

This chapter will be divided into two distinct parts. The first part will be dedicated to the definition of the research question which will guide the developments of this dissertation. In the second part, we will be defining the research hypotheses and explaining how we intend to conduct the researches accordingly.

3.1 Research question.

The development of the European cybersecurity is a complex question where many actors from all backgrounds intervene and interact. The European cybersecurity policies must insure the resilience and security of the European cyber ecosystem while dealing with numerous obstacles such as the increasing politicization of the questions related to cybersecurity at the national level.

The subject of this dissertation is *“the role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of the European cybersecurity”*. As it has been shown in the literature review, the debates among the intellectual community highlight two great considerations on the evolution of the European cybersecurity and the creation of ENISA: the institutionalization of the European cybersecurity policies and the heterogeneity among Member States regarding cybersecurity in term of national cybersecurity institutions and strategies.

The institutionalization of ENISA evolves in a context marked by these two conflicting tensions. In one hand, the expansion of the Information Technologies creates growing threats of diverse natures and origins which calls for a pan-European solution for these problems acting on a rapidly expanding scale. On the other hand, ENISA touches to a relatively new field of national security and many Member States have already adopted many norms and institutions in order to insure their national safety. This relation between institutionalization and Member States ‘normative heterogeneity regarding cybersecurity issues allows the formulation of the following research question:

“How does intergovernmental and supranational interests have influenced the institutionalization of ENISA?”

The term institutionalization must be here understood as the political process by which the principals of ENISA design the institutional form of this agency. Henceforth, the study of the institutionalization of ENISA will comprehend the analysis of the evolution of ENISA’s overhaul organizational structures, control mechanisms, objectives and financial resources allocated to fulfill these objectives as well as the scope of the competences delegated to the agency by the principals.

By intergovernmental interests, we understand the political desires of some of the national and European actors to limit the scope of the competences and the degree of discretion of ENISA. As such, the intergovernmental interests dictate that the role of ENISA in the European cybersecurity policies must be limited and the autonomy of national cybersecurity policies must be insured. Furthermore, this notion of intergovernmental interests also implies that Member States must keep a close political control over ENISA and that the Member States must play the most important role in the political decision-making regarding the institutionalization of ENISA.

Accordingly, the supranational interests can be defined as the political will of certain national and European institutions to broaden the scope of ENISA's competences and to insure that the degree of discretion of this agency can be perceived as high. The political control over ENISA will tend to be loose and ENISA will be free to decide of its own agenda while insuring the deepening of European integration in regard of cybersecurity policies.

3.2 Research hypotheses.

In order to answer the research question of this dissertation, we will formulate two research hypotheses.

1. *The European Parliament and the Council of the European Union are the two principals of ENISA. The European Parliament tends to advocate for a supranational agenda while the Council of the European Union tends to defend an intergovernmental agenda.*

This first research hypothesis will allow the analysis of the balance of power between intergovernmental and supranational interests during the legislative debates regarding the creation of ENISA's act of delegation. The European Parliament and the Council are the two main institutions intervening in the debates during the ordinary legislative procedure. The choice of studying these two institutions specifically is thus relevant because the regulations forming ENISA's act of delegation are being produced accordingly to the ordinary legislative procedure.

From a theoretical perspective, this hypothesis will be studied under the lens of the principal-agent's notion of politics of delegation. Consequently, we will study the equilibrium in terms of influence between the European Parliament and the Council on the design of ENISA's act of delegation. As the notion of politics of delegation dictates, this hypothesis will be solved solely by studying the political negotiations at the highest level of European politics and not by analyzing the internal functioning of the ENISA.

In order to formulate a practical answer to this hypothesis, we will study the documents linked to the different stages of the legislative debates related to the conception of ENISA's act of delegation. In this regard, we will be analyzing the debates surrounding the creation of the 2004

regulation⁵⁵ as well as the 2008 regulation⁵⁶, the 2011 regulation⁵⁷ and the 2013 regulation⁵⁸ to understand the influence of the European Parliament and the Council on the institutionalization of ENISA. The debates regarding the upcoming 2018 regulation⁵⁹ will also be analyzed as it will be intellectually interesting to assess the evolution of the equilibrium between supranational and intergovernmental influences in the institutionalization of ENISA by comparing the debates regarding the conception of these different regulations and the 2018 regulation even though this text hasn't enter in force yet.

2. The management board of ENISA is the main control mechanism set by the principals and defends intergovernmental interests.

This second hypothesis will allow us to take a closer look on how intergovernmental influences may impact the internal functioning of ENISA as an agency. The management board is one of the most central decision-making institutions within the agency. This board is constituted by persons affiliated to the Union, national institutions or even the civil society to take important decisions regarding the functioning, the orientation of the agency's actions, and the allocation of human and financial resources to the agency's projects or even in the nomination of executive directors of the agency.

Accordingly, the composition of the management board and the voting rules, defined in the act of delegation of the agency, are paramount in the functioning and the degree of discretion of an agency as the management board may serve the interests of one specific kind of European or national actor.

The analysis of ENISA's management board will be conducted accordingly with the principles of the principal-agent theory's notion of politics of discretion. Henceforth, the analysis will only regard the internal functioning of ENISA and we will be assessing the influence of the management board on the degree of discretion of ENISA.

In order to conduct this analysis of the importance of the role of the management board on ENISA's internal functioning and to evaluate the intergovernmental influences on the management board, we will study the sociological composition of the management board. Furthermore, we will be interested in the voting rule of the management board and how they have evolved with the different reforms of ENISA's acts of delegation. Finally, we will study the influence of the management board by inspecting the minutes of the management board's meetings and evaluating the influence of this meeting on ENISA's internal functioning.

⁵⁵ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, No 460/2004.

⁵⁶ Council of the European Union and the European Parliament, *Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 28 September Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2008, L 293/1.

⁵⁷ Council of the European Union and the European Parliament, *Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2011, L 165/3.

⁵⁸ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, No 526/2013.

⁵⁹ European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2017, 2017/0225(COD).

Chapter 4: ENISA and the European cybersecurity policies.

The European Network and Information Security Agency (ENISA) has been founded in 2004 and has only grown in importance for the European cybersecurity landscape ever since. As it will be soon presented, ENISA has many missions but its core activity is to insure the prevention of the risks induced by an economy more and more dependent on Information and Communication Technologies. As the digitalization of the economy is a well-established trend and as the number of connected objects are only becoming more and more important in the everyday life of the European citizens, 86 percent of the citizenry believes that the risk of being a victim of cybercrimes is more important today than it ever was in the European Union⁶⁰.

More importantly, recent historical events have shown the lack of preparation of the European States and institutions in front of a major cybersecurity incidents. The 2007 cyberattack on the internet infrastructures of the Estonian government⁶¹ or the 2011 cyber aggression on the European institutions⁶² have highlighted the importance of the development of a strong European cybersecurity framework.

In a society and in an economy which are always more connected, the development of good cybersecurity practices concerns every level of governance. Cybersecurity policies have to insure the European consumers' confidence in the digital market while maintaining a sufficient level of security regarding the critical infrastructures of the member states. This particular blend of consumer protection and of national security is the main difficulty in the policy-making of European cybersecurity policies.

As we will see in the next part of this dissertation, the 2013 European cybersecurity strategy⁶³ have shaped the European cybersecurity policies in three distinct parts: cyber criminality, Network and Information Security (referred as NIS) and cyber defense. These three policies are affected by diverse degree of European integration and this dissertation will be focused on the NIS policy.

As a central actor of the NIS policy, the mandate of ENISA is determined by this tension between the need for European harmonization, the safety of the fragmented European digital market and the imperatives dictated by the national security of the Member States. Henceforth, ENISA must fulfill a wide variety of missions from insuring the safety of the European consumers as well as preparing the critical infrastructures of entire Member States in the event of a major cyber incidents.

In order to give a comprehensive study of ENISA as an agent of the European Union, this chapter will be divided in several part. The first part will introduce briefly the European cybersecurity landscape and will show the influence of the 2013 European cyber strategy in the formation of the different European cybersecurity policies. The second part of this chapter will

⁶⁰ European Commission, *Eurobarometer 464a: Europeans' Attitudes towards Cyber Security*, Brussels, 2017, 464a, pp.56.

⁶¹ The Guardian, Russia accused of Unleashing Cyberwar to Disable Estonia, the guardian, <https://www.theguardian.com/world/2007/may/17/topstories3.russia>, consulted on the 12/07/2018.

⁶² EUobserver, EU institutions hit by « major » cyber-attack ahead of summit, EUobserver, <https://euobserver.com/news/32049>, consulted on the 12/07/2018.

⁶³ European Commission, *Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions-Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyber space*, Brussels, 2013, JOIN (2013) 1 final.

discuss the role of ENISA as an agency and the evolution of its missions in regards of the changes regarding the regulations defining its mandates and the reforms in the NIS policy.

4.1 The European cybersecurity policies: a fragmented landscape.

Cybersecurity is a recent concern for the European institutions. In Europe, the events of Tallinn in 2007 served as a wake-up call. During the month of April 2007, tensions rose between the Russian and Estonian governments over a controversy regarding an historical landmark celebrating the liberation of Tallinn by the Soviet army in 1944. Angered by the Estonian political choices, the Russian government retaliated by launching a series of cyber-attack on the internet infrastructures of the Estonian political and economic institutions. This event, one of the first of its kind, triggered reactions within NATO and the European Union leading to the institutionalization of proper policies regarding cybersecurity⁶⁴.

Today, if the institutionalization of cybersecurity policies has resulted in positive changes, cyber threats are still evolving and a great number of different actors, Public and private alike, may cause harm on a global scale with different methods and means. For example, in 2013, it has been estimated that the yearly gain of cybercriminals around the world was of 750 billion euros⁶⁵.

One of the most fascinating aspects of cybersecurity, as a policy field, is that it is a product of its era. Unlike many other aspects of security, cybersecurity policies have been a priority only since the beginning of this century and, as a result, have been developed both on the National and European level with little interest for coherence. As such, European cybersecurity policies have been created to work in synergy with the national cybersecurity policies and to ease the coordination between the multiple national, European and international actors involved in the European cybersecurity landscape. Nevertheless, the Member States' cybersecurity policies are extremely diverse and the emergence of a common doctrine or institutional layout, which could create a dynamic of convergence regarding cybersecurity practices among Member States, struggles to appear in Europe.

As such, Distrust and normative heterogeneity among the national cybersecurity actors hampers the functioning of the European cybersecurity⁶⁶ in its whole. The 2013 European cyber strategy⁶⁷ gave the foundation of the current layout of the different European cybersecurity policies. The 2013 cyber strategy describes three structural axis organizing the European cybersecurity landscape: the cyber defense policy, the cyber criminality policy and the NIS policy. We will briefly describe the first two policies and we will give a more in-depth analysis of the NIS policy in order to present the very particular role of ENISA in the European cybersecurity landscape.

⁶⁴ The Guardian, Russia accused of Unleashing Cyberwar to Disable Estonia, the guardian, <https://www.theguardian.com/world/2007/may/17/topstories3.russia>, consulted on the 12/07/2018.

⁶⁵ European Commission, *Commission Staff Working Document: Assessment of the EU 2013 Cybersecurity Strategy*, Brussels, 2017, SWD (2017) 295 Final, p.6.

⁶⁶ Ibidem, p. 26-30.

⁶⁷ European Commission, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions-Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyber space*, Brussels, 2013, JOIN (2013) 1 final.

4.1.1 The 2013 European cyber strategy: an approach in three axis.

The European cyber criminality and cyber defense policy illustrate well the diversity of the different axis of the European strategy in term of integration at the European level and of organizational and operational autonomy. In this regard, the European cyber defense policy is considered to be the less institutionalized of the three branches.

But first and foremost, it is important to notice that an organizational principle guides the structure of the three branches of the European cybersecurity strategy. A fundamental trait of the organization of the three branches is the strict separation between the European level of institutions, where actors such as ENISA operate, and the national level, where a vast variety of public and private actors act. The European governance of the cybersecurity policies is thus characterized by the European cybersecurity institutions guiding the cooperation of complex networks of national cybersecurity institutions. The Union is here essentially an agent of convergence and regulation insuring an efficient level of cooperation between the numerous actors involved in cybersecurity policies and, as such, the European level of cybersecurity institutions doesn't hold comprehensive operational powers even though this level of operational powers may vary from one branch of the European cyber strategy to another⁶⁸.

As an axis of the European cyber strategy, the European cyber defense policy doesn't have a dedicated agency but relies on different European bodies to achieve the objectives of the 2013 European cyber strategy. The European cyber defense policy depends from the Common Security and Defense Policy (CSDP)⁶⁹.

The European cyber defense policy aims at enhancing the cyber defense capabilities of the Member States while insuring an efficient level of coordination at the European level through the use of CSDP missions and the cooperation between European and national institutions with NATO. Accordingly, there is a few institutions which are responsible of the conduct of the European cyber defense policy even though there mandates only concern cyber defense indirectly for most of them.

The first important aspects of the contemporary cyber threats is there hybrid nature. Tackling the issue of cyber defense, and cybersecurity at large, means involving civilian and military actors alike. As such, a first priority of the European cyber defense policy is to insure the build-up of cyber defense capabilities at the national level by developing good practices and expertise within the civilian and military actors assigned to the cyber defense by the national strategies but also insure that these civilian and military actors work in synergy in order to insure the highest level of efficiency. The actors responsible at the European level are here the European Defense Agency (EDA) but also agencies which are not directly linked with defense policies such as ENISA or the European Cybercrime Center (or EC3). These agencies insure that a common level of protection standards is reached throughout the Union⁷⁰.

⁶⁸ CHRISTOU, George, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Hampshire, Palgrave Macmillan, 2016, p.1-3.

⁶⁹ European Commission, *Commission Staff Working Document: Assessment of the EU 2013 Cybersecurity Strategy*, Brussels, 2017, SWD (2017) 295 Final, p.43-46.

⁷⁰ Ibidem, p.36-40.

The cooperation at the European level depends of the willingness of the Member States to act voluntarily within the framework of CSDP missions. However, the recent developments regarding the Permanent Structured Cooperation (PESCO) have allowed a more in-depth cooperation between Member States creating opportunities to share expertise in regard of cyber defense issues at the European level. Nevertheless, the cooperation within the framework of PESCO are still based on the willingness of the States to join these programs and, thus, doesn't represent a fully-fledged European cyber defense cooperation⁷¹.

Ultimately, NATO stays the milestone of the cyber defense cooperation for the Member States and establishing a close cooperation with NATO is one of the main objectives of the European cyber defense policy accordingly to the 2013 cyber strategy⁷². In conclusion, the European cyber defense policy stays a concern for the European leadership but the lack of directly concerned European agents, the importance of NATO in the European cooperation in regard of cyber defense coordination and the intergovernmental decision-making demonstrate that the European cyber defense policy stays the less developed branch of the European cybersecurity landscape.

Inversely, the European cyber criminality policy represents the most operational branch of the European cybersecurity landscape. As it was stated earlier in this text, cyber criminality is a vicious and growing phenomenon that may harm the confidence of companies and citizens in the digital economy. Accordingly, the European cybercriminal policy have been designed to achieve a high degree of operational efficiency⁷³.

Depending on DG Home, the three main actors of the European cybercriminal policy are the European Police Office (Europol), Eurojust and the more recently created European Cybercrime Center (EC3). Europol⁷⁴ is an agency created in 2010 in order to ease police forces cooperation within the Union. EC3⁷⁵ is a subdivision within Europol charged to act as a nexus for all of the actors affected by cybercriminal issues. Accordingly, EC3 must give operational supports to national cybercrime authorities, to ease cooperation between different Member States cybercrime authorities but also to prevent cybercrime itself by researching and diffusing good practices for the European citizens, companies and the national as well as the European institutions. This role in the prevention of cybercrime through the diffusion of good practices is also shared by ENISA. Eurojust is the other European agency regarding the European cyber criminality policy and essentially insure the convergence of legal practices regarding cybercrime throughout the Member States.

EC3, Eurojust and Europol are meant to work together in close cooperation in order to lift the obstacles hampering the judicial cooperation among Member States and third countries on the issues related to cyber criminality. In this regard, the cooperation between these three

⁷¹ European Union External Action website, Permanent Structured Cooperation (PESCO)-factsheet, https://eeas.europa.eu/headquarters/headquarters-homepage/34226/permanent-structured-cooperation-pesco-factsheet_en, consulted on 12/07/2018.

⁷² European Commission, *Commission Staff Working Document: Assessment of the EU 2013 Cybersecurity Strategy*, Brussels, 2017, SWD (2017) 295 Final, p.44-46.

⁷³ Ibidem, P.11-16.

⁷⁴ Europol, About Europol, Europol website, <https://www.europol.europa.eu/about-europol>, consulted on the 12/07/2018.

⁷⁵ Europol, European Cybercrime Center-EC3, Europol website, <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>, consulted on the 12/07/2018.

institutions have been considered as being remarkably efficient and the cyber criminality branch of the European cyber strategy is extremely active.

Essentially, national safety and the importance of high politics in the Member States' decision-making can be understood as the main deciding factors of differences between the three branches of the European cybersecurity landscape in term of operability at the European level. While Cyber criminality policies remain somewhat low-politics and call for an active participation at European level in order to achieve the objective of curtailing European cyber criminality sets by the national preferences, the development of national cyber defenses is still a highly politicized question and the Member States prefer to keep a firm control over these competences or to cooperate through international organizations perceived as being more legitimate in regard of security issues, such as NATO.

The development of the European NIS policy, as the third pillar of the European cyber strategy, has been characterized by the tension created by the importance of low-politics and high-politics questions in the preferences of the Member States as the European NIS policy, and its institutions, have authorities over several key aspects of national cybersecurity policies.

4.1.2 The Network and Information Security policy.

The article 4 of 2004 regulation regarding the mandate of ENISA give this definition of the concept of Network and Information Security:

“network and information security means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems”⁷⁶

As such, the European NIS policy aims at insuring the safe use of Information and Communication Technology (ICT) within the European single market. Moreover, the NIS policy encompasses an extremely diverse number of missions concerning different layers of power within the Union as the scope of competence of the NIS policy touches the European consumers, the national institutions and the European institutions alike. If the applications of the NIS policy are extremely diverse, two logics inside this policy can however be identified⁷⁷.

Firstly, the economic logic has dominated the development and institutionalization of the NIS policy. The development of a unified European digital market, the importance of creating a growing European digital industry and insuring the confidence of the European consumers in the digital economy have been key missions of the European NIS policy⁷⁸.

As it will be soon presented, ENISA has played an instrumental role in this matter. The production of guidelines and good practices for the industries or European consumers and the introduction of European certifications regarding ICT goods and services have been some of

⁷⁶ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1, article 4, p.5.

⁷⁷ CHRISTOU, George, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Hampshire, Palgrave Macmillan, 2016, p.119-120.

⁷⁸ Idem.

the core activities of ENISA in regard of the economic logic governing the European NIS policy⁷⁹.

Furthermore, the European institutions have always been careful to encourage the different stakeholders of the digital economy to participate in the development of the different aspects of the NIS policies. The doctrine of multi-stakeholderism is thus actively pursued within the framework of the NIS policy as the different important actors of the European digital economy are being represented in different organs of European NIS institutions. For example, in ENISA, the Permanent Stakeholder's Group assists the Executive Director and the Management Board in the governance of the agency⁸⁰.

Secondly, the security logic has been instrumental in the development of the NIS policy. The notion of security is different in regards of NIS policies as the absence of threats and dangers is impossible to achieve in a cyber ecosystem. As such, the European legislator has decided to conceptualize security as cyber resilience. In a 2011 report, ENISA defines the notion of Cyber resilience as *"the ability to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation"*⁸¹. As such, the recovery of a compromise system and insuring a minimum cybersecurity threshold sufficient to suppress the eventual cyber threats and incidents is here more important than preventing the existence of these threats itself⁸².

In this regard, the security logic of the NIS policy encompasses a vast amount of mission as it is not only the cybersecurity of the consumers' digital devices that must be insured but also the cybersecurity of all of the critical infrastructures throughout the Union. Accordingly, the NIS policy aims at insuring the cybersecurity of the national and European institutions along with the cybersecurity of the critical infrastructures of the Member States such as the energy grids or the logistical nodes among many examples⁸³.

In this context where there is such a vast number of critical infrastructures to protect, the main characteristic of the European NIS dispositive is its decentralization and its ability to function as a complex network of cybersecurity national and European institutions. As such, there is vast number of different doctrines and types of institutions insuring cybersecurity throughout the different Member States of the Union. The 2016 NIS directive was the most significant steps taken at the European level to insure a minimum level of harmonization amongst the different national approaches of cybersecurity that have been developed so far by the Member States. In this regard, the 2016 NIS directive marks an historical evolution of the European governance on NIS policy as the Union takes a much more proactive role on this matter.

⁷⁹ European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2017, 2017/0225(COD).

⁸⁰ Council of the European Union and the European Parliament, Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004, Brussels, 2013, L 165/41, article 12.

⁸¹ ENISA, *inter-X: Resilience of the Internet Interconnection Ecosystem*, Athens, 2011, 18th, April 2011(b), p.16.

⁸² CHRISTOU, George, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Hampshire, Palgrave Macmillan, 2016, p.141.

⁸³ European Commission, *Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*, Brussels, 2016, L 194/1, annex II.

The 2016 NIS directive has created new institutions and insured the adoption of minimal standards of cybersecurity at the national level while influencing dramatically the mandate and role of ENISA in the European cybersecurity landscape. The first major change brought by the directive was the obligation for the Member States to adopt national cybersecurity strategies and to create at least one national Computer Security Incident Response Team (CSIRT) in charge of the cybersecurity on key institutions and critical infrastructures. A CSIRT's network has been created at the European level in order to insure the cooperation and coordination amongst the different national CSIRT and the Computer Emergency Response Team guarding the European institutions (CERT-EU)⁸⁴.

Furthermore, the Member States must establish a list of operators of essential services⁸⁵ which will be strategic in the event of cyber incidents. These essential operators can be identified as being part of seven different strategical sectors defined in the annex of the NIS directive⁸⁶: the energy sector, the transports sector, the banking sector, the financial market infrastructures, the health sector, the water infrastructures and the digital infrastructures.

In order to achieve the implementation of all of the measures dictated by the NIS directive, a group of cooperation has also been created to promote the coordination and cooperation among Member States as well as the trust among the different actors involved in the European cybersecurity⁸⁷.

Nevertheless, if the NIS policy covers a vast array of questions and competences regarding key aspects of the European security and economy, a comprehensive number of compromises were made during the development of the NIS policy which hamper the functioning of this policy and of its agents in order to insure the autonomy of national security.

For example, if the NIS directive establishes the obligation of creation of at least one national CSIRT and national cybersecurity strategy per Member State, however the organizational form, or number, of the national institutions assimilated to a CSIRT are not defined within the NIS directive leaving a broad autonomy to the Member States in this matter⁸⁸. Furthermore, the national cybersecurity strategy has to be available at the European level but the Member States may choose to dissimulate parts of their national strategies if they judge that these parts of their strategies are too sensitive to be shared at the European level⁸⁹.

Another example of compromise can be seen in regard to the nomination of essential operators at the national level. Indeed, the Member States are not supposed to inform the European institutions of their list of essential operators but only to explain the methodology used to designate these operators as a proof that the Member States have complied with this provision of the NIS directive⁹⁰.

⁸⁴ European Commission, *Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, Brussels, 2016, L 194/1, article 9.

⁸⁵ *Ibidem*, article 5.

⁸⁶ *Ibidem*, annex II.

⁸⁷ *Ibidem*, article 11.

⁸⁸ *Ibidem*, article 9.

⁸⁹ *Ibidem*, article 7.

⁹⁰ *Ibidem*, article 5.

These few examples are only contained in the NIS directive but illustrate well the shortcoming of the NIS policy. These functional flaws, purposely created within the framework of the NIS policy, institutionalized the lack of homogenization of the different doctrines and institutions responsible for the national and European cybersecurity while creating voluntarily information asymmetries between the different cybersecurity institutions. Conclusively, these shortcomings, conceived to preserve the autonomy of the Member States in regard of their national security policies, hamper the operability of the European NIS policy at a supranational level. ENISA, which can be considered as the heart of the European cybersecurity dispositive, has known a complicated development and institutionalization due to the fact that the NIS policy is fundamentally the child of a consensus between supranational necessities and intergovernmental interests.

4.2 The European Network and Information Security Agency.

Created in 2004⁹¹, the European Network and Information Security Agency (ENISA) has been ever since its creation the central node and milestone of every aspects of the European NIS policy and its security and economic components. Alike to the NIS policy, the development of ENISA, as an agency, has been extremely complex and several periods through the agency's history can be identified where the role of ENISA has known comprehensive changes.

In this part, we will identify this period of mutation and concentrate ourselves on defining the objectives of ENISA while describing the different means used by the agency to comply with these objectives. But first of all, we will present the legal basis of ENISA's mandate and the controversy surrounding the legal basis chosen by the European legislator.

4.2.1 A legal basis under the article 95 TEC/ 114 TFEU: a controversial choice?

As the two first regulations governing ENISA's mandate have been introduced prior to the amendments of the Treaty of the European Community (TEC⁹²) changing it as the Treaty on the Functioning of the European Union (TFEU⁹³) in 2009, the article 95 TEC⁹⁴ was the legal basis of the 2004 regulation⁹⁵ and the 2008 regulation⁹⁶. Meanwhile, the 2011 regulation⁹⁷ and

⁹¹ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1.

⁹² Official journal of the European Community, *Consolidated Versions of the Treaty on European Union and of the Treaty Establishing the European Community*, Brussels, 2002, C 325/1.

⁹³ Official Journal of the European Union, *Consolidated Version of the Treaty on the Functioning of the European Union*, Brussels, 2008, C 115/47.

⁹⁴ Official journal of the European Community, *Consolidated Versions of the Treaty on European Union and of the Treaty Establishing the European Community*, Brussels, 2002, C 325/1, article 95.

⁹⁵ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1.

⁹⁶ Council of the European Union and the European Parliament, *Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 28 September Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2008, L 293/1.

⁹⁷ Council of the European Union and the European Parliament, *Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2011, L 165/3.

the 2013 regulation⁹⁸ as well as the future regulation⁹⁹ defining the mandate of the ENISA had, for legal basis, the article 114 TFEU¹⁰⁰ as the alternative to the article 95 TEC.

Even though the choice of the article 95 TEC/114 TFEU may seem relatively harmless, using this article as a legal basis for the 2004 regulation has caused a severe disagreement among the Member States which will find its conclusion in a ruling of the European Court of Justice (ECJ). The case C-217/04¹⁰¹ has opposed the United Kingdom to the European Parliament and the Council of the European Union.

In this case, the United Kingdom contested the validity of the article 95 TEC as the legitimate legal basis of the 2004 regulation and argued that the article 308 TEC¹⁰² was a more legitimate legal basis for the regulation. Henceforth, the United Kingdom asked for the annulment of the 2004 regulation which would mean the dissolution of the recently-created ENISA¹⁰³.

The United Kingdom observed that the article 95 TEC was used to harmonize national laws and didn't had the power to install community bodies. Furthermore, the British explained that ENISA, due to its role as an NIS adviser, didn't have the authority to influence directly the national legislations regarding national NIS policies. As such, the true purpose of ENISA was to reduce the fragmentation of the European digital market rather than to harmonize the existing national legislations¹⁰⁴.

Additionally, ENISA had for competence and objective the creation of a cybersecurity culture common through the European Union. The United Kingdom viewed this competence as being beyond the scope of the article 95 TEC and, thus, beyond the competences of the Union to harmonize the European single market. As such, the article 308 TEC should have been more legitimate as it was dedicated to the situations where European actions were necessary to the functioning of the European single market but where the Union didn't had any competences to act accordingly to the European treaties¹⁰⁵.

Ultimately, the ECJ ruled in favor of the European Parliament and the Council of the European Union and, as a consequence, the article 95 TEC, or its alternative the article 114 TFEU, stayed the legal basis of the 2004 regulation and any regulation defining the mandate of ENISA ever since. Nevertheless, a change of legal basis for ENISA would have modified entirely the balance of power between the European Parliament and the European Council as the article 114 TFEU is associated with the ordinary legislative procedure described at the article 294 TFEU¹⁰⁶ which

⁹⁸ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41.

⁹⁹ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD).

¹⁰⁰ Official Journal of the European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, Brussels, 2008, C 115/47, article 114.

¹⁰¹ European Court of Justice, *Case C-217/04: United Kingdom of Great Britain and Northern Ireland against the European Parliament and the Council of the European Union*, Kirchberg, 2006, C-217/04.

¹⁰² Official journal of the European Community, *Consolidated versions of the Treaty on European Union and of the Treaty Establishing the European Community*, Brussels, 2002, C 325/1, article 308.

¹⁰³ European Court of Justice, *Case C-217/04: United Kingdom of Great Britain and Northern Ireland against the European Parliament and the Council of the European Union*, Kirchberg, 2006, C-217/04, p.1.

¹⁰⁴ Ibidem, p.10-11.

¹⁰⁵ Ibidem, p.12.

¹⁰⁶ Official Journal of the European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, Brussels, 2008, C 115/47, article 294.

allows both institutions an equilibrate role in the legislative procedure regarding ENISA's regulations. A change to Article 308 TEC, or its alternative the article 352 TFEU¹⁰⁷, would had left the Council with a unanimity based voting procedure and the European Parliament with a simple consultative or approbation role depending on which treaty is in force.

During the fifth meeting of ENISA's management board on the 11 March 2005¹⁰⁸, the use of the article 95 TEC over the article 308 TEC were extensively discussed among the members of the management board representing the different Member States. During the meeting, the UK representative appeared isolated and the others Member States' representatives seemed to have reached a consensus on the use of the article 95 TEC. However, the case C-217/04 proved that, at the beginning of ENISA, the foundation of a NIS agency had been viewed as controversial and some Member States judged that it would have been more preferable if ENISA had been put under the scope of article 308 TEC allowing a stronger intergovernmental control over the agency in the foreseeable future. The legitimacy of the use of article 95 TEC/114 TFEU hasn't been questioned ever since.

4.2.2 The evolution of ENISA's missions and tasks.

The history of ENISA has been marked by the transformation of the missions of the agency as the NIS policy itself changed in term of complexity and operability. Accordingly, ENISA's tasks have evolved with the changes of regulations governing ENISA's mandate. As such, we will be analyzing the changes brought by the 2004 regulation, the 2008 regulation, the 2011 regulation and the 2013 regulation. For the sake of completion, the future changes brought by the soon-to-be new regulation on ENISA's mandate will also be presented as well.

The 2004 regulation will set the core activities of ENISA for at least the next decade. ENISA was to be a hub of experts creating a common European NIS culture by sharing the agency's expertise and linking every European actors, private as public or national as European alike, important to the European cybersecurity landscape and participating in the external action of the European Union in regard of NIS policy.

In practice, the objective of ENISA will be translated in a number of tasks. A first example of tasks of ENISA will be to promote awareness and best practices to all of the relevant actors in front of the diverse dangers susceptible to be inflicted to Network and Information System. As such, ENISA was actively collecting data and doing risk assessment in order to develop risk management procedures and advised the different actors on the development of best practices in prevention and risk management¹⁰⁹.

Establishing a close link between the industry, the national institutions and the European Commission was another great task of ENISA. Advising the Commission on the development of NIS practices and technologies was an explicit objective of the agency¹¹⁰. The idea was to increase the readiness of every actors in case of severe cyber incidents while creating a

¹⁰⁷ Official Journal of the European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, Brussels, 2008, C 115/47, article 352.

¹⁰⁸ ENISA, *Minutes of the Fifth Meeting of the Management Board Held on 11 March in Centre Borschette*, Brussels, 2005, Brussels, Fifth meeting.

¹⁰⁹ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1, article 3.

¹¹⁰ Idem.

“network” logic where the multi-stakeholderism will be fundamental in the development of future NIS policies.

Fundamentally, these tasks had been implemented by several means. Direct advices and supports to actors asking for ENISA’s assistance was always a first option but several more methods of action will soon be developed on the basis of the 2004 regulation such as the future cyber exercises¹¹¹ overseen by ENISA. However, the real core activity of ENISA was the production of reports and guidelines on the basis of analysis conducted on NIS related practices. As such, the operations of ENISA were decided in advance in work programmes which were vividly discussed by the different institutions in charge of ENISA’s supervision.

The 2008 and 2011 regulations only expanded the ENISA’s mandate in term of time but their elaborations allowed some key debates on the future of ENISA’s mandate and functions. One of the defining aspects of ENISA as an agency was that ENISA’s mandate was limited. Originally, the 2004 regulation only gave ENISA a 5 years mandate¹¹². Meanwhile, the 2008 regulation added 3 years¹¹³ to this mandate and the 2011 regulation expanded further ENISA’s mandate with 1.5 years¹¹⁴. This limitation on ENISA mandate will be continued in the 2013 regulation with ENISA’s mandate being limited to 7 years from the 19 June 2013¹¹⁵. The new regulation¹¹⁶ on ENISA’s mandate should be the first regulation to grant ENISA an unlimited mandate.

The question of the limited mandate is primordial to understand the relations between ENISA and the Member States. As it is stated in the tenth meeting of the management board (22-23 March 2007)¹¹⁷, the limitation of ENISA’s mandate was essentially a consensus between the Member States supporting the creation of a NIS agency and the Member States which were not in support of such idea. Creating a commune European NIS culture can only be a long-term project, as such discussing the duration of the agency itself would lead inevitably to discuss the scope of the competences of this agency itself. Conclusively, the periods preceding the adoptions of the 2008 and 2011 regulations were rich in debates on the future of the ENISA and the operational role of this agency.

It was the first time that ideas such as the product certification¹¹⁸ were openly debated but will only become an integral part of ENISA’s activities a decade later. Meanwhile, the first cyber Europe exercise was conducted in 2010¹¹⁹ and these exercises will soon become an important

¹¹¹ ENISA, *Cyber Europe 2010-Evaluation Report*, Heraklion, 2011.

¹¹² Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1, article 27.

¹¹³ Council of the European Union and the European Parliament, *Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 28 September Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2008, L 293/1, article 1.

¹¹⁴ Council of the European Union and the European Parliament, *Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2011, L 165/3, article 1.

¹¹⁵ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 36.

¹¹⁶ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD).

¹¹⁷ ENISA, *Minutes of the 10th Management Board Meeting*, Heraklion, 2007, 10th meeting.

¹¹⁸ ENISA, *Minutes of the 9th Management Board Meeting*, Heraklion, 2007, 9th meeting.

¹¹⁹ ENISA, *Cyber Europe 2010-Evaluation Report*, Heraklion, 2011.

asset in preparing the European cybersecurity actors to an eventual pan-European cyber incident. Conclusively, if the 2008-2011 period introduced some key ideas on what kind of agency ENISA would be in the near future. However, ENISA will have to wait the 2013 regulation to see real changes in its mandate.

The 2013 regulation must be understood in its historical context. The 2013 regulation is closely linked to the introduction of many political choices made at the European level to push forward the European agenda on cybersecurity related policies. As such, the 2013 regulation must be examined under the light of the 2013 cyber strategy. Accordingly, if the 2013 regulation is essentially based on the missions described in the 2004 regulation, ENISA will now be more involved in the implementation and operationalization of European decisions at the national level. The role of ENISA in the build-up of cybersecurity policies throughout the Union was reaffirmed specially regarding the development of national CSIRT.

The 2013 regulation was introduced in a period of transition for the NIS policy as soon after the 2016 NIS directive entered in force and greatly expanded the role of ENISA as the agency became instrumental in the creation of national CSIRT and national cyber strategy made mandatory by the NIS directive. Furthermore, the role of ENISA as an advisor to the European institutions was reinforced by the creation of the CSIRT's network and the cooperation group¹²⁰.

Similarly to the 2013 regulation, the future regulation on ENISA's mandate will also expand the scope of ENISA's missions as the agency will soon produce certification for ICT goods and services in order to resorb the fragmentation of the European single market on this matter¹²¹.

It must be noticed that the 2013 regulation and the new regulation also change drastically the way the internal affairs of ENISA are being conducted. As it will be presented in this dissertation, the 2013 regulation has changed how the internal organs of ENISA worked and has eased the Commission's control over the agency while the upcoming regulation will grant ENISA an unlimited mandate.

The specificity of these two regulations is that they have been introduced when the legal framework for NIS policy was changed dramatically by the introduction of the NIS directive¹²² and the 2013 cyber strategy¹²³. As such, if the missions of ENISA have been defined by these regulations, the real legal authority of the ENISA can be found in the NIS directive and the 2013 cybersecurity strategy due to some of the mandatory provisions of these texts such as the creation of national CIRST and national cybersecurity strategy where ENISA's involvement is necessary.

¹²⁰ European Commission, *Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, Brussels, 2016, L 194/1.

¹²¹ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD).

¹²² European Commission, *Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, Brussels, 2016, L 194/1.

¹²³ European Commission, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions-Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyber space*, Brussels, 2013, JOIN (2013) 1 final.

Conclusively, the role of ENISA has known substantial changes since the beginning of the 2010 decade sparking debates within the management board which are still unresolved to this day. With ENISA gaining operational powers as the agency plays an instrumental role in the development of national and European cybersecurity institutions or with the development of European ICT certification, is ENISA still only a center of expertise or an operational agent at the heart of the European cybersecurity landscape? And if ENISA have received substantial operational powers, is the agency ready to assume the responsibility of its new missions? Since the twenty-third management board meeting on the 21 March 2013¹²⁴, the question of operational powers versus expertise is regularly discussed in the management board as the Member States representatives debate if ENISA's staff is qualified for these new missions or if the actual budget of the agency is enough to fulfill these missions. As the European NIS policy changed in past few years, ENISA's role have mutated and all of these questions regarding these changes haven't been answered yet.

¹²⁴ ENISA, *23th Management board meeting*, 2013, Heraklion, MB/23/10.

Chapter 5: ENISA's internal institutions and control mechanisms.

With the framework of the action of ENISA defined, the internal institutions of ENISA will now be analyzed and the control mechanisms set by the principals will be described. The role played by ENISA's internal institutions and the control mechanisms set by the European legislator are closely linked as the nomination of the agents constituting these institutions and the dynamics between these institutions are key elements of potential control mechanisms.

By internal institutions, we understand the institutions described in the different ENISA's regulations which play an instrumental role in the internal-decision making of the agency. As such, the activities of the executive director and of the management board will be presented and analyzed. A sociological study of these actors will also be conducted as far as the sources available will allow it. In order to conduct a thorough analysis, the control mechanism set to monitor the use of financial resources will also be studied.

This chapter will be divided in several parts. The first part will explain how the analysis conducted in this chapter relates to the principal-agent theory. The second part will analyze the actions of the executive director. The third part will be focused more deeply on the management board as it is the key institution of the internal functioning of ENISA. The fourth part will describe the allocation of budgetary resources to the agency. The fifth and final part will conclude this chapter by synthesizing the analysis of the different control mechanisms set by the European legislator.

5.1 ENISA and the politics of discretion.

The analysis conducted in this chapter will follow the principles described by the notion of politics of discretion¹²⁵ developed within the principal-agent theory. Knowingly, the analysis will concern the formal and informal control mechanisms set by the act of delegation defining the relationship between ENISA, as the agent, and its principals and how these control mechanisms define the balance of power between ENISA and its principals.

In this case, the diverse regulations defining ENISA's mandate will be considered as being acts of delegation establishing the relationship between ENISA and its principals. Henceforth, the 2013 regulation¹²⁶ is the act of delegation currently in force even though the other regulations will be considered in the analysis in order to establish if there is dynamics in the balance of power between the different institutions involved in the internal functioning of ENISA.

Due to their importance in the making of the regulations defining ENISA's mandate, the European Parliament and the Council of the European Union will be both considered as being the main principals of ENISA as the regulations are being adopted under the ordinary legislative procedure where both of these institutions hold a considerable influence. The role of the European Commission is here far more ambiguous as this institution is involved in the ordinary legislative procedure, regarding the elaboration of ENISA's regulations, but has also a direct role in the internal functioning of ENISA. The Commission can be then considered as having

¹²⁵ ADRIAENSEN, Johan, DELREUX, Tom, "Introduction. Use and Limitations of the Principal-Agent Model in Studying the European Union", in ADRIAENSEN, Johan, DELREUX, Tom (Dir.), *the Principal Agent Model and the European Union*, Basingstoke, Palgrave Macmillan, 2017, p. 18-22.

¹²⁶ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41.

acquired a mandate with ENISA's regulation and, thus, can be viewed as an agent of the Council and the European Parliament creating effectively a chain of delegation between the principals having created the regulation, the Council, the European Parliament and the Commission, and then the agent monitoring several aspects of ENISA's internal functioning, the European Commission, and finally the ENISA as an agent itself.

5.2 The executive director.

The executive director of ENISA is the top management officer of the agency. He/She plays a central role in the day-to-day management of the agency and exercises a decisive influence on the orientation of the agency on the medium and long term. Beyond his/her managerial activities, he/she is charged to apply the decisions taken by the management board in regard to budgetary matters and of the implementation of the works programmes defining the annual operations of the agency¹²⁷.

The executive director is also in charge of the trans-institutional communication as he/she must answer the questions of the European Parliament and of the Commission on a regular basis. Furthermore, he/she is explicitly responsible for the good communication with the stakeholders and, thus, insures that the industry is being consulted and benefits from ENISA's actions¹²⁸. As such, he/she chairs the permanent stakeholder's group which is an internal institution of ENISA charged to establish a relationship between the agency and the stakeholders of the industry¹²⁹.

More practically, the executive director is in charge of producing strategic documents on a yearly basis which will be adopted or amended by the management board and communicated to the European Parliament, the Council and additional institutions depending on the nature of the documents such as the court of auditors for budgetary documents or the European Economic and Social Committee as well as the Committee of Regions for other documents before publication.

Three categories of documents can be distinguished. Firstly, the annual, or less commonly multi-annual, work programmes¹³⁰ are produced by the executive director in order to plan the operations and objectives of ENISA. The work programme must first be submitted to the Commission for consultation and then transferred to the management board for a vote or an amendment. This procedure is currently in force and detailed in the 2013 regulation and should stay sensibly the same in the new upcoming regulation¹³¹, however, this procedure has been more monitored by the European institutions in the 2004 regulation. During the 2004 regulation's procedure, the European Parliament and the Council were also consulted before the publication of these documents¹³².

¹²⁷ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 14.

¹²⁸ *Idem*.

¹²⁹ *Ibidem*, article 12.

¹³⁰ *Ibidem*, article 13.

¹³¹ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD), article 21.

¹³² Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1, article 7.

The second category of documents produced by the executive director is a budgetary report accounting the yearly revenues and expenditures of the agency. The budget will be submitted to the management board for adoption and adjustments and then will be sent to the Commission and the rightful financial institutions to be examined. If the budget is in order, it will be then integrated to the general budget of the Union¹³³.

It is here important to notice that the executive director is responsible for the financial good governance of the agency. The balance between the expenditures and the revenues of the agency must always be balanced¹³⁴ and the executive director must cooperate closely with institutions such as OLAF in order to prevent frauds. After the 2013 regulation, the executive director must also develop and implement an anti-fraud strategy within the agency with the assistance of OLAF¹³⁵.

The third document produced by the executive director is the general report presenting the situation and progress of ENISA during the year preceding the publication of the document¹³⁶. In the 2013 regulation, the general report must only be submitted to the vote or amendments of the management board but this report was far more scrutinized under the 2004 regulation as the European Parliament, the Council, the Commission, the Economic and Social Committee and the Committee of Region were supposed to be informed of this document¹³⁷. Evidently, this document used to serve as an evaluation of the utility of ENISA as, in the earliest year of the agency, some European and national actors didn't fully support the idea of a NIS agency.

These documents are instrumental in the orientation of ENISA's action and some of them, specifically the work programmes, give the executive director a substantial autonomy in the choices related to ENISA's future actions and role as an agent of the European cybersecurity. It is important to notice that the monitoring of the European institutions regarding these documents has been greatly reduced between the 2004 regulation and the 2013 regulation. Indeed under the 2004 regulation, each document had to be, at the very least, submitted to the European Commission for consultation. Under the 2013 regulation and onward, the work programmes and the general report are no longer monitored by any European institution, at least formally, and only submitted to the vote or amendments of the management board. As such, the European institutions have lost potent *ex ante* control mechanisms on ENISA as the agency is formally free to decide and implement its work programmes.

If the control of the European institutions has been reduced over time in this regard, the appointment procedure of the executive director is still under firm European control. The candidate for the post of executive director is chosen by the management board on the basis of a list of candidates proposed by the European Commission. The candidate nominated by the management board, before its final appointment, shall then answer the questions of the European Parliament and of the Council. It is also important to notice that the management

¹³³ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 19.

¹³⁴ *Ibidem*, article 19 paragraph 4.

¹³⁵ *Ibidem*, article 20.

¹³⁶ *Ibidem* article 11.

¹³⁷ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1, article 7.

board may also remove the executive director but this procedure has never been launched nor considered¹³⁸.

In the 14 years of existence of ENISA, only two executive directors served. The term of office of ENISA's executive director is 5 years¹³⁹ and the eventuality of renewal of this term of office is not mentioned in the regulations. However, one of the executive directors, Udo Helmbrecht, had his mandate renewed¹⁴⁰ so this practice could be considered as accepted.

The first executive director of ENISA was an Italian named Andrea Pirotti¹⁴¹. He was in office between September 2004¹⁴² and October 2009¹⁴³ effectively serving a full five years term. The official sources give little information about him except that he originated from an important telecommunication company called Marconi Communication. As such, he came from the industry and was clearly specialized in the implementation of projects regarding advanced IT infrastructures. Presumably, he was chosen for the post of ENISA's executive director for his expertise and his managerial skills rather than for political reasons.

The second executive director, a German named Udo Helmbrecht, served two terms beginning in October 2009¹⁴⁴ and will still be in office presumably until October 2019. He played an important role in the development of ICT in private German companies between 1985 and 2003 and then served as the president of the German federal office for information security between 2003 and 2009 before becoming the executive director of ENISA. Accordingly, it is fair to assume that he has experience both with the industry and with the national ICT institutions¹⁴⁵.

Conclusively, if the executive director plays an important role as a pivotal institution in the communication between the ENISA's decision-making institutions, such as the management board, or ENISA's principals and the day-to-day management of the agency, the appointment of the executive director doesn't seem to obey political imperatives but seems to be objectively based on the expertise and management skills of the candidate. As such, the appointment procedure itself could be seen as a control mechanism set by the European institutions but doesn't seem to hinder the discretion of the agency in regard of its activities or the practical orientations of its missions decided in the work programmes.

¹³⁸ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 24.

¹³⁹ *Idem*.

¹⁴⁰ ENISA, *ENISA Management Board Extraordinary Meeting: 11 September 2014 Rome, Italy*, Heraklion, 2014, 24/09/2014.

¹⁴¹ European Commission, *European Network and Information Security Agency Up and Running*, site of the European Commission, <https://ec.europa.eu/digital-single-market/en/news/european-network-and-information-security-agency-and-running>, consulted on the 12/07/2018.

¹⁴² ENISA, *Minutes of the Second Meeting of the ENISA management Board Held on the 14-15 September*, Heraklion, 2004, ENISA_MB/EL/JB/01_Draft.

¹⁴³ ENISA, *Minutes of the 16th ENISA Management Board Meeting*, Heraklion, 2009, 16th meeting.

¹⁴⁴ *Idem*.

¹⁴⁵ ENISA, Udo Helmbrecht-Curriculum Vitae, ENISA's website, <https://www.enisa.europa.eu/about-enisa/structure-organization/executive-director/udo-helmbrecht-cv/view>, consulted on the 12/07/2018.

5.3 The management board

Although the executive director has a strategic role in overseeing ENISA's activity, it is the management role which plays the most important role in ENISA's internal decision-making and the control of the European institutions over the agency.

The management board discusses every aspect of ENISA's functioning. The debates between the members of these institutions concern the rules governing the missions, the budget, the staff's nomination and the future orientation of ENISA's operational actions. Even in regard of the aspects of ENISA's governance where the management board has no authority upon, the debates of this assembly hold a vast influence on the actors responsible on these matters. As such, the executive director is questioned, judged and receive advices at every meetings of the management board.

Conclusively, the management board is the most natural institution to impose formal and informal control mechanisms on ENISA and every legal and practical aspect of the management board's functioning is instrumental to determine the degree of discretion enjoyed by the agency.

5.3.1 Composition, meetings, voting procedures of the management board.

Under the 2004 regulation's layout, the management board was composed by one representative per Member States and an alternative to this representative was to be appointed in case of if the national representative couldn't be present at the meeting. Three representatives were also nominated by the Commission and three other representatives of the civil society representing the consumers and the industry were present at the meetings. Under this configuration, every representatives had the right to vote except the three representatives of the civil society¹⁴⁶.

The 2013 regulations introduced slight changes to the voting procedure as the number of representatives of the Commission were reduced from 3 to 2 and the posts of the representatives of the civil society were simply suppressed. As a consequence, the 2013 regulation confirmed a balance of power strongly in favor of the Member States for the control of the management board and the upcoming regulation shouldn't change the management board's voting procedure¹⁴⁷.

The absolute majority voting rule applies in the Management board but the qualified majority voting rule (2/3 of the votes in favor) is being applied on several occasions. Indeed, the rules of procedure governing the debates within the management board, the internal rules of operation of the agency, the budget, annual and multiannual work programmes and the nomination of the executive director or the management board's chairperson, a representative elected among his peers to govern and set the date of the meetings, are decided on the basis of the qualified majority vote procedure¹⁴⁸. However, akin with the voting procedure in the Council, the

¹⁴⁶ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1, article 6.

¹⁴⁷ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 6.

¹⁴⁸ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 9.

decision-making of the management relies almost exclusively on the consensus of its members as negative votes are practically inexistent during the meetings.

The European Commission used to be the most important actor regarding the production of rules in the management board. The agency's internal rules of operation, the management board's rules of procedure used to be only proposed solely by the Commission under the 2004 regulation and the Commission was to be consulted on the adoption of the work programmes or the financial rules¹⁴⁹. This strain on the management board's autonomy has been reduced with the 2013 regulation as the initiative regarding these documents were granted to the Management Board. The Commission was then consulted only for the internal rules of operation and the procedure rules¹⁵⁰. As such, the changes between the 2004 regulation and the 2013 regulation regarding the voting rules and the adoption of decisions prove that the European institutions have reduced dramatically the control mechanisms on ENISA's institutions.

It is also worth mentioning that the regularity of the meetings was modified between the regulations. As such, two ordinary meetings were to be organized per year by the chairperson accordingly to the 2004 regulation¹⁵¹ while the 2013 regulation¹⁵² declared that only one ordinary meeting per year was to be set. The upcoming regulation¹⁵³ should revert this change however as two ordinary meetings should happen per year when the regulation will come in force. Extraordinary meetings can also be organized on the basis of a decision from the chairperson or a demand of at least a third of the representatives. These extraordinary meetings were only organized four times in ENISA history and the decisions related to this meeting were taken in regard of the election of a new chairperson¹⁵⁴, the renewal of the mandate of the executive director Udo Helmbrecht¹⁵⁵ or amendments regarding a work programme¹⁵⁶.

The regulations don't introduce any rules for the nomination of the representatives by the Member States or the Commission. However, the 2013 regulation¹⁵⁷ specifies that the Commission and the Member States should prevent any excessive turnover of the representatives. Evidently, the representatives of the management board are encouraged to be long term members of this assembly and evidence suggests that this rule has been so far respected by the different actors. For example, the Austrian representative, Reinhard Posch, have been present from the first meeting to the most recent meeting serving 14 years in a row in ENISA's management board.

¹⁴⁹ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1, article 6.

¹⁵⁰ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 5.

¹⁵¹ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1, article 6.

¹⁵² Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 8.

¹⁵³ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD), article 16.

¹⁵⁴ ENISA, *ENISA Management Board Extraordinary Meeting*, Athens, 2013, MB/2013-E/2.

¹⁵⁵ ENISA, *ENISA Management Board Extraordinary Meeting: 11 September 2014 Rome, Italy, Heraklion*, 2014, 24/09/2014.

¹⁵⁶ ENISA, *Draft Minutes of Extraordinary Meeting of the Management Board of ENISA Held on the 20 July 2017*, Brussels, 2017, 20/07/2017.

¹⁵⁷ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 6.

The sociological profile of the representatives chairing at the management board is also interesting in order to assess the influence of ENISA's management board on the agency discretion. The current management board (set on the 28 May 2018¹⁵⁸) is composed of high ranking officers from the Member States and Commission. The two representatives of the Commission, and their alternates, represent respectively the DG CONNECT and the DG DIGIT¹⁵⁹ but the Member States' representatives have a far more influential role due to their far more important number.

The profiles of the Member States' representatives are more diverse than the one of the Commission's representatives. Their profiles ranged from an executive director of a national CERT/CSIRT to the member of a minister's cabinet but all of them are somewhat close to the national authorities responsible for the development and implementation of national NIS policies. The greatest divide among the national representatives is between the ones working for national executive or regulatory NIS agencies and the others working in national administrations or ministerial departments. The distribution between these groups is, however, quite even as 14 representatives are coming from national administrations or departments against 13 from national agencies. Accordingly, 10 of the alternates come from an administrative background against 11 from national agencies. Furthermore, in most of the cases, it didn't seem to be a clear hierarchical difference between the representatives and their alternates¹⁶⁰.

In conclusion, ENISA's management board is formally dominated by the representatives of the Member States thanks to the composition of the assembly and the sheer weight of the national representatives in the voting procedure. The strong national influence in the management board suggests a strong national and intergovernmental control of the agency.

5.3.2 The Management board's internal debates.

The voting rules and the composition of the management board tend to support the idea that the management board is instrumental in the intergovernmental control of the agency. However, if the structure of the assembly itself encourages the influence of the Member States on ENISA, the reality of the debates conducted in this institution could lead to a different conclusion.

The management board debates on every aspect of ENISA's functioning. Most of the management board's activities are actually spent debating on the executive director's management of the agency. As such, the discussions on the work programmes issued by the executive director dominate every meeting and are the most regularly discussed documents.

The importance of the work programmes must be highlighted as these documents are instrumental in the conduct of ENISA's actions. Essentially, the work programmes decide what kind of operations will be led the following year and which NIS matters will be analyzed by the experts of the agency¹⁶¹. In this regard, the management board has on several instances taken important decisions on the design of these documents by asking the executive director to base

¹⁵⁸ ENISA, *List of ENISA Management Board Representatives and Alternates*, Heraklion, 2018, 24.05.2018.

¹⁵⁹ *Idem*.

¹⁶⁰ *Idem*.

¹⁶¹ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 13.

the future work programmes on an output approach rather than on a topical approach¹⁶², among many other examples. The management board has also the authority to advise the executive director to prioritize certain aspects of the work programmes if the assembly judges that the subjects are irrelevant or that the resources of the agency are spread too thin to tackle them efficiently¹⁶³.

Obviously, the finances of the agency are discussed by the management board and, more specifically, the documents linked to the agency's budget are debated and regularly amended. Nevertheless, these questions are often less addressed than the work programmes and were only extensively addressed on March 2011¹⁶⁴ when the agency had difficulties to balance its revenues and its expenditures. The administration of the agency's staff is also discussed but the debates on this matter are closely linked with the debates on the agency's financial state.

The regular activities of the agency are more freely discussed during the yearly report of the executive director to the management board on the state of ENISA's affairs. The minutes of the management board make it clear that the executive director is accountable to the management board even though the assembly never took restrictive actions against any of the two executive directors.

Beyond the usual debates on the governance of the agency, the management board also discusses on determining subjects such as the future of the European NIS policies and the place of ENISA in these policies. In this regard, the management board is determinant in the design of the agency's role in the European cybersecurity landscape. A prime example of the management board influencing the operational priorities of the agency can be found on the debate following the appointment speech of the executive director Udo Helmbrecht on the 15-16 October 2009¹⁶⁵.

During the debate, Udo Helmbrecht argued that ENISA's priority was to insure the security of the European consumers and, thus, the agency's focus should be set on the economic aspects of ENISA's governance by encouraging the IT industry in Europe. The management board's representatives didn't discourage this orientation but advised caution and noticed that the development of the cooperation between the Member States, regarding cybersecurity, was one of the most pressing objectives of the agency. Finally, the assembly noted that it wasn't in the management board that ENISA's future was decided but in the Council of the European Union¹⁶⁶.

The exchange can be enlightening on several levels. First of all, it illustrates the fact that the management board acts as an *ex ante* and *ex post* control mechanism on the executive director and on the agency, by extension, through him. The management board recommends its operational choices to the executive director and the director knows that he will be accountable before the agency for his choices as the head of ENISA. Arguably, it could also suggest that the real power of the management board is psychological as no sanctions have ever been taken

¹⁶² ENISA, *Minutes of the Seventeenth ENISA Management Board Meeting*, Heraklion, 2006, 17th meeting.

¹⁶³ ENISA, *Minutes of the 16th ENISA Management Board Meeting*, Heraklion, 2009, 16th meeting.

¹⁶⁴ ENISA, *Minutes of the 19th ENISA Management Board Meeting*, Heraklion, 2011, 19th meeting.

¹⁶⁵ ENISA, *Minutes of the 16th ENISA Management Board Meeting*, Heraklion, 2009, 16th meeting.

¹⁶⁶ *Idem*.

against the executive director and yet the authority of the assembly seems to be respected by him.

Secondly, this example illustrates the relationship between the management board and its principals, the European institutions. Throughout the 32 minutes of the management board published over more than 14 years, a parallelism can be noted between the European institutions and the management board even though the relations are obviously quite cordial. This is mostly due to the fact that, even if the management board is the most influential institution in regard of ENISA's internal functioning, the assembly doesn't have any influences on the legislative procedure ultimately deciding of ENISA's existence.

Udo Helmbrecht's appointment debate is only one among many examples of occasions where the management board discussed the future of ENISA in the European NIS policy. Since the 2013 regulation, many debates have also irrupted on ENISA's capabilities to respect its mandate specifically in regard of its new operational missions such as the assistance to the setup of national CERT, national cybersecurity strategy or ICT services and goods certification¹⁶⁷. Some representatives doubt that ENISA will have the human and financial resources to achieve all of these new tasks while retaining a satisfactory level of efficiency.

Ultimately, the recent developments regarding ENISA's missions have been a challenge to the management board's governance because one of the main goals of this assembly has been to keep ENISA respectful of its mandate. With a broadened mandate, the management board may find it harder to define ENISA's core mission while the role of the agency is being severely modified and expanded by the European principals.

In conclusion, the representatives of the management board's debates haven't served to limit the agency's influence or to insure that the execution of ENISA's mandate will not overlap with the duties of national cybersecurity institutions. The main of achievement of this assembly was to keep ENISA in the mandate that had been defined by the principals in the different regulations. Thanks to the analysis of the debates of the management board, we can conclude that the main preoccupations of the representatives were to insure the functional efficiency of the agency, within the framework of its mandate, rather than imposing an intergovernmental or supranational control over ENISA.

5.4 Financial and budgetary resources.

The final control mechanisms studied in this chapter will be related to the allocation of financial resources to ENISA. It has been established that, since the 2013 regulation, ENISA has a growing number of responsibilities and tasks in regard of the implementation and development of European and national cybersecurity policies. Meanwhile, the resources available to ENISA had always been deemed limited by the actors in direct contact with the agency¹⁶⁸.

ENISA was the product of a consensus between the Member States which wished for a European NIS agency and the Member States which didn't had the same preferences¹⁶⁹. As

¹⁶⁷ ENISA, *European Network and Information Security Agency Management Board Meeting*, Athens, 2015, 2015/10/21-22.

¹⁶⁸ ENISA, *23rd ENISA Management Board Meeting*, Heraklion, 2013, MB/23/10.

¹⁶⁹ ENISA, *Minutes of the 10th Management Board Meeting*, Heraklion, 2007, 10th meeting.

such, it is more than fair to assume that the Member States were somewhat reluctant to invest important funds into an agency which could exist only temporarily due to its limited mandate. As it will be shown, ENISA's budget has been expanded over time with each new regulation signaling an increase in the financial resources available to the agency.

In 2004, the year of the foundation of the agency, the budget was of 3.500.000¹⁷⁰ euro but the budget will be consolidated in 2005 by rising to 6.800.000 euro¹⁷¹. The 2008 regulation will grant a budget increase to 8.416.928 euro¹⁷². Finally, the year 2016, which coincides with the NIS directive, will bring ENISA's budget to 11.060.564 euro¹⁷³. In all the periods in between these dates, ENISA's budget was stable with some slight variations. In comparison, the budget of Europol, the European law enforcement agency, had on the same 2016 period a budget of 102.242.000 euro¹⁷⁴.

The adoption of ENISA's budget and its implementation is a heavily monitored process and, even though these aspects of ENISA's governance have been presented on the part related to the executive director, should be presented more thoroughly. ENISA's revenue sources are the subsidies given by the European Union, the contribution of non-European States which have benefited from ENISA's actions and, since the 2013 regulation, the voluntary contributions of the Member States¹⁷⁵.

On the month of March of any given year of activity of ENISA, the Executive director will present a draft statement of the revenues and expenditure of the agency for the following year to the management board which will then transfer the document to the Commission. After analysis, the Commission will send the document to the European Parliament and the Council along with the preliminary general draft of the general budget of the European Union.

In the 2004 regulation, the Commission determines the subsidies granted to ENISA in the preliminary general draft of the general budget of the Union¹⁷⁶. In the 2013 regulation however, it is the role of the European Parliament and the Council to authorize the subsidies which are the first income sources of the agency¹⁷⁷.

Finally, the final draft of the agency budget is sent to the management board to be approved as soon as possible. The implementation of the agency's budget is also a well monitored process as ENISA's accounting officer has to transfer the agency's account details to the Commission's accounting officers who have here the same authority as on any components of the Commission itself. The Commission's accounting officers then send the account details to the Court of

¹⁷⁰ ENISA, *2005 Budget*, Heraklion, 2005, 2005 budget, p.4.

¹⁷¹ Idem.

¹⁷² ENISA, *2008 Budget*, Heraklion, 2008, 2008 budget, p.4.

¹⁷³ ENISA, *2016 Budget*, Heraklion, 2016, 2016 budget, p.4.

¹⁷⁴ EUROPOL, *Statement of Revenue and Expenditure of the European Police Office for the Financial Year 2016 — Amending Budget No 2*, La Haye, 2016, 2017/C 84/36, p.2.

¹⁷⁵ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 19.

¹⁷⁶ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1, article 15.

¹⁷⁷ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 19.

Auditors which, in turn, will send the details and its observations to the European Parliament and the Council¹⁷⁸.

Finally, the executive director, on the basis of the analysis of the agency's accounts details, will present to the management board his plans for the implementation of ENISA's recently adopted budget. The management board will then send back the executive director's proposition to the European Parliament, the Council, the Commission and the Court of Auditors¹⁷⁹.

With all these procedures, anti-frauds policies have been progressively implemented in the European agencies with OLAF becoming an influential player in the financial control of the agency. The executive director, the management board and the ENISA accounting officer were then charged to implement an anti-fraud strategy in the agency¹⁸⁰ under the supervision of OLAF.

The financial control of ENISA involved a large array of European and ENISA's institutions in a dynamic and thorough process. Nevertheless, the institutions of the European *trias politica* occupied the most important place in the political control of the agency's financial management and the limited financial resources of the agency have been a recurrent problem in the agency's administration.

This limitation on ENISA's financial resources makes the role of the management board and the governance of the executive director extremely important in the internal functioning of the agencies as the management board has on several instances chosen to prioritize particular aspects of ENISA's work programmes in favor of others¹⁸¹. Most notably, the recent debates on the evolution of ENISA's role in the European cybersecurity landscape have also shown that the representatives of the management board are in contact with their respective governments on this subject as some of them, specifically the German representative, have warned the executive director that their countries will not commit more funds to the agency if ENISA would over-spend its budget¹⁸².

5.5 ENISA's discretion and its control mechanisms.

In conclusions, the types and intensity of the control mechanisms characterizing the agency's discretion have known clear evolutions with each ENISA's reforms and regulations passing. The agency is arguably far more autonomous in its 2013 layout than in its 2004 institutional form and the future reforms only seem to reinforce this historical dynamic. Evidently, the initial lack of confidence in certain European and national actors in the idea of a European NIS agency has clearly decreased over time and ENISA is accepted in the current European cybersecurity landscape as a legitimate security actor despite the questions raised by the recent evolutions of its mandate.

A first expression of the progressively acquired confidence is the reduction of the monitoring of documents produced by the management board and the executive director by the different

¹⁷⁸ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41, article 21.

¹⁷⁹ *Idem*.

¹⁸⁰ *Ibidem*, article 20.

¹⁸¹ ENISA, *Minutes of the 16th ENISA Management Board Meeting*, Heraklion, 2009, 16th meeting.

¹⁸² ENISA, *23th Management board meeting*, 2013, Heraklion, MB/23/10.

European institutions. Along with the diminution of the Commission's role in the adoption of the agency's internal procedures and operation rules, the reduction of the interventions of the European institutions between the 2004¹⁸³ and the 2013¹⁸⁴ regulations marks the end of a "trial period" for ENISA and marks the end of the period of implementation of the agency as a European body.

Furthermore, one of the most important control mechanism set since the 2004 regulation, and perpetuated ever since, will be finally suppressed by the new upcoming regulation¹⁸⁵. The question of the limited mandate of ENISA was asked at each debate on new regulations and was a potent psychological control mechanism in regard of the agency's internal functioning and operational choices as, if the agency didn't gave satisfaction to its principals, it could simply disappear due to a deadline set in the document describing its own mandate. The perspective of an unlimited mandate signals that a consensus has been reached by every national and European actor and that ENISA has been deemed efficient and legitimate to the eyes of these actors. Accordingly, we could expect that this change will be translated into more autonomy, thus more discretion, for the agency as ENISA could act more independently, within the framework of its missions, without fears of seeing its mandate not being renewed by its principals.

The financial and budgetary resources' allocation are also a considerable control mechanism since the adoption and the implementation of the budget is a long and complex procedure which is under a heavy monitoring by the Commission, the European Parliament and the Council. However, it could be argued that the whole budget adoption procedure and the obligation to submit financial documents to OLAF is not unique to ENISA and that every European body must be put under such surveillance for the sake of financial orthodoxy and transparency. Nevertheless, ENISA's budget size stays a political decision and, as such, constitutes an operational control mechanisms as the institutions grant funds to the agency on the basis of how they judge the scope and importance of ENISA's mandate.

More surprisingly, the nomination of the executive director and the representatives of the management board seems to be a very low politic process. With the 5 years and the potential renewable mandate of the executive director and the imperative of reducing the turnover of the representatives, the behavior of the actors constituting both of these institutions doesn't seem to be under heavy monitoring of the Member States or of the European principals. However, it could be argued that the real control mechanism is not found in the nomination of these agents but rather in the design of these two institutions as the members of these institutions are themselves hand-picked by the principals on the basis of their expertise and their close relations with national cybersecurity institutions.

As such, the executive director and the management board allow a diffuse control over the internal functioning of the agency as the institutions are central in the management of ENISA

¹⁸³ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1

¹⁸⁴ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41.

¹⁸⁵ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD),

and its decision-making. Conclusively, having representatives being, firstly, member of national institutions and then only, secondly, part-time representatives in the ENISA's management board insures that the assembly, by its composition, will have the preferences of the Member States as a priority when the assembly decides of an important operational decision.

Due to its authority over the executive director and its comprehensive influence over every aspects of the agency's governance, ENISA's management board can be viewed as the main control mechanism set by the principals. By its composition, it is also clear that the agency defends an intergovernmental agenda however it is interesting to see that the operational efficiency of the agency is defended by the management board.

Chapter 6: the legislative debates regarding ENISA's acts of delegation.

As it has been seen in the previous chapter, the internal institutional layout of ENISA has known substantial changes throughout the introductions of the different regulations defining the agency's mandate. This sixth chapter will present how the balance of power between the European institutions involved in the legislative debates regarding these regulations has influenced the institutionalization of ENISA.

Conclusively, this chapter will be focused on the legislative debates regarding the making of the 2004, 2008, 2011, 2013 and the soon-to-be 2018 regulations. Rather than explaining every change made by the European Parliament and the Council during the different trialogues negotiations or readings, this analysis will bear on the priorities set by these institutions and how they were successful in the defense of their interests.

This chapter will be divided in several parts. The methodology and objectives of this chapter will be explained more in detail in the first part. A second part will present the debates surrounding the introduction of the 2004 and 2008 regulations in the earliest stage of ENISA's history. The third part will be focused on the negotiations regarding the 2011 and 2013 regulations. The fourth part will analyze the still unIntroduced 2018 regulation. Finally, a fifth part will offer a general conclusion to this chapter by summarizing the general positions of the European Parliament and the Council in regard of ENISA's mandate and the balance of power during the legislative debates between the two institutions.

6.1 The methodological, theoretical and research aspects of this chapter.

Due to reasons of security and secrecy, accessing documents describing the negotiations on key institutions of the European cybersecurity landscape is not always a simple task. As such, it is important to present the different sources used in this chapter and how these sources were exploited to conduct an analysis of the relationship between the European Parliament and the Council of the European Union during these reforms.

However, before presenting the sources used in this chapter, the next point of this chapter will present the theoretical premises of this chapter and how these theoretical orientations have shaped the objectives of this chapter.

6.1.1 Theoretical considerations: actor-mapping and principals viewed as a collective.

As it was explained in the fourth chapter, the principals of ENISA are the European Commission, the European Parliament and the Council of the European Union. This characteristic of these European institutions, in their relationship with ENISA, can be explained by their roles in the legislative procedures regarding the making of the acts of delegation defining ENISA's mandate, knowingly the regulations¹⁸⁶.

As such, the European Parliament and the Council were recognized as the main principals as they play a more prominent role in the back-and-forth constituting the negotiations on the legislative texts. In this regard, if the Commission has the legal initiative of presenting a

¹⁸⁶ ADRIAENSEN, Johan, DELREUX, Tom, "Introduction. Use and Limitations of the Principal-Agent Model in Studying the European Union", in ADRIAENSEN, Johan, DELREUX, Tom (Dir.), *the Principal Agent Model and the European Union*, Basingstoke, Palgrave Macmillan, 2017, p. 3-6.

regulation and plays a key role in the formal and informal dialogues, the core of the negotiations is the prerogatives of the European Parliament and of the Council¹⁸⁷.

But all of these aspects of the actors-mapping were seen in the fourth chapter. The real addition of this chapter, in regard of the theoretical framework, is the fact that it is vital to consider the principals as being collective actors in the analysis conducted in this chapter. Simply put, a collective actor is an actor constituted by several sub-actors having a will of their own¹⁸⁸. For example, the European Parliament is not only the assembly constituted by the Members of the different European deputies but also the Industry, Research and Energy committee (or ITRE Committee) which is itself constituted by the Members of the European Parliament and the Rapporteur assigned to this committee.

This new layer in the European decision-making signifies that the European institutions are not monoliths driven by a single will but are in fact several actors struggling in order to impose their interests as the official objectives of the European institution of which they are an integral part. Accordingly, the position of an institution can be weakened if the sub-actors constituting it don't agree with each other on the objectives to advocate during the inter-institutional negotiations.

Conclusively, the Commission is actually constituted by different DG that may have conflicting views on the development of ENISA. However, no institution is more divided, in this fashion, than the Council. The Council itself is constituted by the different delegations of the Member States and led by the rotating presidency. To add to the complexity of the negotiations between these 28 national delegations, the Committees of the Permanent Representatives of EU Member States (the Coreper) also represent a further layer of decision-making inside the Council. Accordingly, the Council can be easily divided on specific issues and the effect of this potential disunity will be presented in the next parts of this dissertation.

6.1.2 Sources: availability and types.

A second element necessary to consider before analyzing the negotiations related to ENISA's regulations is the sources exploited for the analysis conducted in this chapter. The five regulations analyzed are to be considered as being an integral part of the 14 years of evolutions and debates regarding the European cybersecurity policies. As such, the types of sources used in this chapter have to be described.

First of all, only the legal texts constituting ENISA's acts of delegation are being considered in this chapter. Henceforth, the only texts and procedures analyzed under this condition are the

¹⁸⁷ Official Journal of the European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, Brussels, 2008, C 115/47, article 294.

¹⁸⁸ ADRIAENSEN, Johan, DELREUX, Tom, "Introduction. Use and Limitations of the Principal-Agent Model in Studying the European Union", in ADRIAENSEN, Johan, DELREUX, Tom (Dir.), *the Principal Agent Model and the European Union*, Basingstoke, Palgrave Macmillan, 2017, p. 3-6.

ones related to the 2004¹⁸⁹, 2008¹⁹⁰, 2011¹⁹¹, 2013¹⁹² and the 2018¹⁹³ regulations. Accordingly, texts instrumental to the evolution of ENISA's mandate, such as the 2016 NIS directive¹⁹⁴ and the 2013 European cyber strategy¹⁹⁵, will not be considered despite their importance.

The documents relevant to the analysis conducted in this chapter are every document related to the legislative procedures regarding the regulations. These documents are the four columns documents describing the informal and formal dialogues, the documents issued within the institutions during the negotiations, the proposal of regulations and their modified versions issued between the different readings.

Eventually, the greatest limitation, in regard of these analyses, are not the types of sources used but rather the scarcity of these documents on several instances. As it has been said ENISA's existence spans over 14 years and is still being actively discussed in 2018, the sources may not be available due to their age or simply because they are still too sensitive in regard of contemporary debates.

Accordingly, data is lacking on several cases. Specifically, key documents regarding the inter-institutional negotiations on the 2004 regulation haven't been digitalized and are thus unavailable. A similar situation can be noticed for the 2018 regulation albeit for totally different reasons. Indeed, negotiations are still being conducted on the new regulation and, even if its introduction is close, most of the documents are too sensitive to be available to a broader audience.

6.2 The 2004 and 2008 regulations.

Every interinstitutional negotiations on ENISA's regulations must be understood in its political context. The creation of a European agency is always a complex political matter and the political debates regarding its formation began long before the formal start of the interinstitutional negotiations on the agency's mandate. For ENISA, the debates and consultations began in 2001 with a communication of the European Commission regarding NIS policies¹⁹⁶.

¹⁸⁹ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, No 460/2004.

¹⁹⁰ Council of the European Union and the European Parliament, *Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 28 September Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2008, L 293/1.

¹⁹¹ Council of the European Union and the European Parliament, *Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2011, L 165/3.

¹⁹² Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41.

¹⁹³ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD).

¹⁹⁴ European Commission, *Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, Brussels, 2016, L 194/1.

¹⁹⁵ European Commission, *Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions-Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyber space*, Brussels, 2013, JOIN (2013) 1 final.

¹⁹⁶ European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Region: Network and Information Security; Proposal for a European Policy Approach*, Brussels, 2001, COM (2001) 298 final.

It was a time following the events of the 11 September 2001 where the vulnerability of critical infrastructures became obvious to the Western World but also where the importance of internet in the economy was only growing stronger and was more and more felt by every political actors. The creation of a European body responsible of NIS matters was the subject of a consensus between the Council, the European Parliament and the Commission. In the month of February 2003, the regulation for the creation of ENISA was proposed¹⁹⁷.

As it was stated in the previous part, key documents are lacking in order to fully understand the interinstitutional debates but it is still possible to understand some of the motivations of the key European actors with the documents which are still available in 2018. First of all, it is clear that the forms and functions of ENISA were thoroughly discussed among the European institutions during the years prior to the proposal.

The documents presenting the 2003 regulation's proposal¹⁹⁸ is extremely close, in its form as in its content, to the definitive version of the regulation signed in March 2004¹⁹⁹. The role of ENISA, and its organizational structure, was remarkably close to the final 2004 regulations. However, it is clear that the introduction of the text is surprisingly enlightening on the ambition of the three principals in regard of the new agency's future. In the span of three pages, the Commission presents the next fifteen years of ENISA's institutionalization. The preparation of national CSIRT, the advisory role on national cybersecurity policies or even the certification of digital goods and services are introduced as being the natural area of authority of ENISA²⁰⁰.

The only element really missing, regarding ENISA's future governance, is the more operational aspects of ENISA's actions. As such, the obligation of the Member States to adopt national cybersecurity policies and national CSIRT as well as the active role of ENISA regarding certification processes are not precisely mentioned in the document. All of these unforeseen changes happened after the 2013 European cyber strategy²⁰¹ and were introduced by the 2016 NIS directive²⁰² and in the 2014²⁰³ as well as 2018²⁰⁴ regulations, which could suggest that a substantial change of philosophy toward ENISA's governance happened in the early 2010' period and allowed a more proactive approach of NIS governance at the European level.

In conclusion, it can be established that the Member States, through the Council, and the Commission had a clear vision of what ENISA meant for the future of the European cybersecurity policies. Nevertheless, substantial changes were made between the Commission's

¹⁹⁷ Commission of the European Communities, *Proposal for a Regulation of the European Parliament and the Council Establishing the European Network and Information Security Agency*, Brussels, 2003, COM(2003) 63 final.

¹⁹⁸ *Idem*.

¹⁹⁹ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, No 460/2004.

²⁰⁰ Commission of the European Communities, *Proposal for a Regulation of the European Parliament and the Council Establishing the European Network and Information Security Agency*, Brussels, 2003, COM(2003) 63 final, p.2-4.

²⁰¹ European Commission, *Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions-Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyber space*, Brussels, 2013, JOIN (2013) 1 final.

²⁰² European Commission, *Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, Brussels, 2016, L 194/1.

²⁰³ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41.

²⁰⁴ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD).

proposal and the adoption. These changes regard the composition and nomination of the management board, the Permanent Stakeholder Group and the scope and tasks of ENISA's mission.

Originally, the management board was supposed to be formed by 14 representatives: 6 nominated by the Council, 6 from the Commission and 2 representing the industry and the consumer²⁰⁵. Later, the ITRE Committee of the European Parliament proposed amendments before the first reading stipulating 5 representatives from the Commission, 5 from the Council, 2 from the European Parliament, 4 from the industry and, finally, 2 representing the consumers²⁰⁶. The definitive version of the 2004 regulation²⁰⁷ allowed for one representative per Member State, 3 from the European Commission and 3 from the civil society. Conclusively, the definitive version shows the Member States gaining clear power over ENISA's most important internal institutions while it is clear that the European Parliament tried to gain a certain measure of formal control over the agency. However, the Commission lost any hope to establish a formal control over this central authority within the agency.

Another noticeable disagreement is the establishment of the permanent stakeholder group. Indeed, while the proposal²⁰⁸ and the ITRE Committee²⁰⁹ proposed the formation of an advisory board, which would have acted more akin to an executive board charged to help the management board and the executive director in the implementation of the agency's decisions, the definitive version created the permanent stakeholder group²¹⁰.

A third area of disagreement is related to the scope and tasks of the agency's governance. Here, the ITRE Committee²¹¹ advocated for a far more extensive description of ENISA's mission and responsibility. However, these changes are less important than it seems because the objectives of the ITRE Committee's rapporteur was here to avoid the ambiguity of ENISA's mandate rather than modify substantially the ethos of ENISA's mission²¹².

At first glance, the most important detail of the negotiations is the vast differences between the amendments proposed by the ITRE Committee²¹³ and the version adopted after the first reading of the European Parliament which was accepted without debates by the Council and then signed by the three principals²¹⁴. Here, the lack of documents forces us to consider two hypotheses. Firstly, the European Parliament implemented comprehensive amendments despite the opinion

²⁰⁵ Commission of the European Communities, *Proposal for a Regulation of the European Parliament and the Council Establishing the European Network and Information Security Agency*, Brussels, 2003, COM(2003) 63 final, article 5, p. 18.

²⁰⁶ European Parliament, *Report on the Proposal of the European Parliament and the Council Establishing the European Network and Information Security Agency (COM (2003)63-C5-0058/2003-2003/0032(COD))*; Committee on Industry, External Trade, Research and Energy; Rapporteur: Reino Paasalinna, Brussels, 2003, A5-0353/2003 (FINAL), p. 17.

²⁰⁷ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, No 460/2004, article 5.

²⁰⁸ Commission of the European Communities, *Proposal for a Regulation of the European Parliament and the Council Establishing the European Network and Information Security Agency*, Brussels, 2003, COM(2003) 63 final.

²⁰⁹ European Parliament, *Report on the Proposal of the European Parliament and the Council Establishing the European Network and Information Security Agency (COM (2003)63-C5-0058/2003-2003/0032(COD))*; Committee on Industry, External Trade, Research and Energy; Rapporteur: Reino Paasalinna, Brussels, A5-0353/2003 (FINAL), 2003.

²¹⁰ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, No 460/2004.

²¹¹ European Parliament, *Report on the Proposal of the European Parliament and the Council Establishing the European Network and Information Security Agency (COM (2003)63-C5-0058/2003-2003/0032(COD))*; Committee on Industry, External Trade, Research and Energy; Rapporteur: Reino Paasalinna, Brussels, A5-0353/2003 (FINAL), 2003, p.5-16.

²¹² Idem.

²¹³ Idem.

²¹⁴ Eurlex, Official Journal of the European Union, volume 47, 13 March 2004, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2004:077:TOC>, consulted on the 04/08/2018.

of the ITRE Committee and the Council accepted accordingly to the codecision procedure²¹⁵. A second hypothesis is that between the consultation of the ITRE Committee and the first reading, an informal trialogue happened and a consensus was set allowing the creation of the definitive version of the 2004 regulation²¹⁶. The second hypothesis might be more fateful to the historical reality than the first one.

On the basis of what is known of the implementation of the 2004 regulation²¹⁷, it is possible to highlight the priorities of the Council and of the European Parliament. As it was stated during the minutes of ENISA's management board²¹⁸, some of the Member States didn't favor the creation of a European NIS agency. As such, it is logical that the political control of the agency by the Member States was an objective of the Council in order to reassure the Member States which were skeptical in regard of the agency's creation. The final version²¹⁹ then allowed the clear control of the agency by the Member States through the composition of the management board at the expense of the Commission and European Parliament. In a way, the doubts of these Member States have reinforced the position of the Council in the negotiation as the qualified majority voting would have allowed these Member States to stop effectively the effort of the Union in regard of the development of a NIS agency.

Through the ITRE Committee's opinion²²⁰, the European Parliament encouraged two aspects of ENISA's mandate. Firstly, the Parliament tried to specify the scope and tasks of ENISA's mission in order to reduce the potential ambiguity of ENISA's mandate and, secondly, to allow the participation of the stakeholders to the agency's governance. The creation of the permanent stakeholder group as well as the modification of the 2004 regulation's first articles were to be the direct translation of these amendments. As such, the European Parliament had forfeited its control of ENISA's management board in order to advance its own view of what should be ENISA's mission. This surrendering, from the Parliament, of the formal control over the agency in order to push its agenda on ENISA's missions and tasks was to become an established trend during the future negotiations.

With the 2004 regulation²²¹, ENISA had a five year mandate to convince its principals of its importance. During this period, the establishment of the agency itself had to be achieved and the skeptical Member States had to be reassured. In this regard, a first step was made with the case C-217/04²²² insuring the validity of ENISA's legal basis and somewhat participating to the reinforcement of the positive consensus among Member States regarding ENISA's existence as

²¹⁵ Official Journal of the European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, Brussels, 2008, C 115/47, article 294.

²¹⁶ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, No 460/2004.

²¹⁷ *Idem*.

²¹⁸ ENISA, *Minutes of the Fifth Meeting of the Management Board Held on 11 March in Centre Borschette*, Brussels, 2005, Brussels, Fifth meeting.

²¹⁹ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, No 460/2004.

²²⁰ European Parliament, *Report on the Proposal of the European Parliament and the Council Establishing the European Network and Information Security Agency (COM (2003)63-C5-0058/2003-2003/0032(COD))*; Committee on Industry, External Trade, Research and Energy; Rapporteur: Reino Paasalinna, Brussels, A5-0353/2003 (FINAL), 2003.

²²¹ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, No 460/2004.

²²² European Court of Justice, *Case C-217/04: United Kingdom of Great Britain and Northern Ireland against the European Parliament and the Council of the European Union*, Kirchberg, 2006, C-217/04.

the minutes of the management board can testify²²³. The negotiations regarding the 2008 regulation²²⁴ began in this context.

The 2008 regulation²²⁵ had one objective: to extend ENISA's mandate in order to allow a more constructed debate on the agency's future and the development of the European cybersecurity policies. There was a clear consensus among the three principals that an extension of mandate was necessary and that the dissolution of ENISA could have represented a great loss for the European NIS policy²²⁶.

The Commission's initial positions mentioned a two year extension of mandate and the creation of a European Electronic Communications Market Authority under which ENISA would have been subordinated²²⁷. Early on, the Council has dismissed the idea of a market authority and had proposed three years of extension instead of the two proposed by the Commission. The ITRE Committee agreed with the Council's position²²⁸.

It is worth mentioning that if the Council managed to create a clear position quickly during the negotiations, Denmark, the United Kingdom and Malta announced that they were scrutinizing the legislative debates regarding ENISA because they felt that their interests could be threatened in regard of the agency's development²²⁹. Henceforth, the distrust of some Member States wasn't quelled by the European Court of Justice's decision related to the case C-217/04²³⁰.

6.3 The 2011 and 2013 regulations.

The 2008²³¹ and 2011²³² were introduced for the same reasons: In order to give more time to the debates regarding the future of ENISA and of the NIS policy, the mandate of ENISA needed to be prolonged. However, unlike the 2008 regulation, the 2011 regulation were issued as an emergency measure and were presented by the Commission on the same day as the proposal for the 2013 regulation²³³. As such, on the 30 September 2010, the proposals for the 2011 and 2013 regulations were introduced and submitted to the interinstitutional debates.

Conclusively, the logic behind the 2008 and 2011 regulations is sensibly the same. However, what was the implicit objective of the 2008 regulation, knowingly to allow a reform of ENISA,

²²³ ENISA, *Minutes of the Fifth Meeting of the Management Board Held on 11 March in Centre Borschette, Brussels*, 2005, Brussels, Fifth meeting.

²²⁴ Council of the European Union and the European Parliament, *Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 28 September Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2008, L 293/1.

²²⁵ *Idem*.

²²⁶ Council of the European Union, *Communication from the Commission to the European Parliament and the Council on the evaluation of the European Network and Information Security Agency (ENISA)*, Brussels, 2007, 10340/07.

²²⁷ Commission of the European Communities, *Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, 2007/0291 (COD).

²²⁸ Council of the European Union, *Preparation of the Transport/ Telecommunications and Energy Council of 12 and 13 June 2008: Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration- General Approach*, Brussels, 2008, 9768/08, p. 2.

²²⁹ *Idem*.

²³⁰ European Court of Justice, *Case C-217/04: United Kingdom of Great Britain and Northern Ireland against the European Parliament and the Council of the European Union*, Kirchberg, 2006, C-217/04.

²³¹ Council of the European Union and the European Parliament, *Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 28 September Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2008, L 293/1.

²³² Council of the European Union and the European Parliament, *Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2011, L 165/3.

²³³ European Commission, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)*, Brussels, 2010, COM (2010) 521 final.

became the explicit goal of the 2011 regulation. An extension of a year and a half was accepted without much debates between the principals²³⁴. The actors feared that the dissolution of ENISA, due to its mandate's temporal end, would have created a legal void in the future European cybersecurity landscape which will be soon presented in the 2013 European cyber strategy²³⁵.

As such, if the 2011 regulation didn't create a stern evolution in ENISA's mandate or in the interinstitutional debates, this regulation marks the beginning of an era of almost continuous debates on ENISA's role and the development of the NIS policy. Nevertheless, the extension of mandate would present an incertitude in the debates concerning the 2013 regulation as the 2011 regulation extended ENISA's existence to the 14 September 2013²³⁶. The 2013 regulation was signed on the 21 May 2013²³⁷.

The principals had a 1.5 years period to negotiate the changes brought by the 2013 regulation and this lack of time was to be felt and noticed by the actors during the negotiations. The most active period of interinstitutional negotiations was between June and December 2012 as three distinct dialogues happened during this period and would result in an agreement based on several compromises on key point of the regulation²³⁸.

The main characteristic of these negotiations was that both the European Parliament and the Council held firm their positions on several key points of the proposed regulation. As such, the negotiations remained somewhat blocked on key aspects of ENISA's governance and these conflicts were unsolved until the last moment of the negotiations or the intervention of another text issued by the European authorities.

The different evaluations of ENISA, under its 2004 regulation layout²³⁹, stated that a first issue of the agency was the managerial difficulties regarding its internal functioning²⁴⁰. These difficulties were caused by two different causes. Firstly, ENISA headquarters was stationed in Heraklion on the island of Crete which was a remote location in regard of the agency's functions in the European cybersecurity landscape. Secondly, the general functioning of ENISA tended to cause managerial slowness which called for a reform in order to streamline ENISA's internal functioning.

The agency location was to become a long standing issue and the relocating of the agency in Athens was finally agreed outside the scope of the regulations' negotiations. During the

²³⁴ Eurlex, Official Journal of the European Union, Volume 54, 24 June 2011, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2011:165:TOC>, consulted on the 04/08/2018.

²³⁵ European Commission, *Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions-Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyber space*, Brussels, 2013, JOIN (2013) 1 final.

²³⁶ Council of the European Union and the European Parliament, *Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2011, L 165/3.

²³⁷ Eurlex, Official Journal of the European Union, Volume 56, 18 June 2013, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2013:165:TOC>, consulted on the 04/08/2018.

²³⁸ Eurlex, Document 32013R0526, procedure, <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex:32013R0526>, consulted on the 04/08/2018.

²³⁹ Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, No 460/2004.

²⁴⁰ Commission of the European Communities, *Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, 2007/0291 (COD).

interinstitutional negotiations on the 2013 regulation²⁴¹, the European Parliament advocated a soft position on this matter allowing ENISA to install offices in diverse locations while the Council tended to support a more conservative position by not allowing ENISA to move out of Heraklion. Strangely enough this issue stayed until the very end of the trialogues' negotiations and was solved by a compromise. ENISA was granted the right to create an office in Athens but would keep Heraklion as its official location²⁴².

The evolution of the ENISA's internal institutions were also extensively discussed in this regard. As such, the missions, scope and tasks related to the agency's mandate were modified to allow ENISA to give advice on the creation of national cybersecurity strategies and national CSIRT. The ITRE Committee of the European Parliament agreed but proposed to develop extensively the description of these missions without betraying the initial ideas of the proposal. If the Council, after several discussions, seemed to accept the ITRE Committee's position, the presidency of the Council imposed that the execution of ENISA's tasks were to be put under the condition that the Member States needed to give their consent to ENISA's actions before the intervention of the agency in national cybersecurity matters²⁴³.

On the subject of ENISA's internal functioning, the propositions of the European Parliament were the most discussed and were the most controversial during the negotiations. Firstly, the ITRE Committee proposed the creation of an executive board which would assist the executive director and the management board on the implementation of European and agency's decisions²⁴⁴. The Council signaled its opposition to this proposition until the last trialogue because it feared that such internal institutions would worsen the managerial difficulties of the agency²⁴⁵. This question, along with many other peripheral questions on ENISA's internal functioning, would be solved by the introduction of the 2012 common approach on decentralized agencies²⁴⁶ which would give a standardized model of decentralized model. This model solved many debates plaguing the interinstitutional negotiations and the idea of an executive board was accepted by the Council albeit with a role far more reduced than the ITRE Committee first proposed²⁴⁷.

The second controversial proposition of the ITRE Committee gave the European Parliament a greater political control over ENISA's management board and executive director²⁴⁸. The candidate chosen by the management board for the post of executive director was to be confirmed by the European Parliament before of his nomination. In a similar fashion, the candidate for the post of chairperson of the management board was to be questioned by the

²⁴¹ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-trialogues document*, Brussels, 2012, 11330/12, p.72.

²⁴² *Ibidem*, p. 2-25.

²⁴³ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-Preparations for the informal Trialogues with the European Parliament*, Brussels, 2012, 15994/12.

²⁴⁴ *Ibidem*, p.43.

²⁴⁵ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-Preparations for the Informal Trialogues with the European Parliament*, Brussels, 2012, 16872/12.

²⁴⁶ Council of the European Union, *Evaluations of the European Union Agencies-Endorsement of a Joint Statement and Common Approach*, Brussels, 2012, 11450/12.

²⁴⁷ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-trialogues document*, Brussels, 2012, 11330/12.

²⁴⁸ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-trialogues document*, Brussels, 2012, 11330/12.

European Parliament and an opinion was issued by the Parliament afterwards. Before the nomination, the management board was supposed to take this opinion into account. The European Parliament would also insure a stricter control of the agency by questioning regularly the executive director on several aspects of the agency's governance.

By the end of the negotiation, the European Parliament had to forfeit their propositions of political control over ENISA's internal institutions but had gained the insurance that the Parliament's concerned committees would be informally consulted on the nomination procedure of the executive director²⁴⁹.

Another great controversy was the ITRE Committee's proposition to allow ENISA to create administrative agreements with third countries in the framework of its external governance and international cooperation with other international organizations²⁵⁰. The Council wasn't keen to grant ENISA too much autonomy on its external governance despite the fact that it was one of these missions. The propositions was withdrawn before the end of the negotiations²⁵¹.

The last long standing issue during the interinstitutional negotiations was the details regarding the extension of ENISA's mandate in its duration. The initial proposition of the Commission was 5 years²⁵². The ITRE Committee proposed 7 years²⁵³ before readjusting on the Commission's position and accepting 5 years²⁵⁴. The Council didn't manage to set an official position before the very last stage of the negotiations accepting the 5 year mandate. This indecision was due to the divergent positions within the Council and the 5 year solution was accepted because it was the most consensual solution accepted by the majority of the actors²⁵⁵. Conclusively, the Council was still disunited on key questions regarding ENISA's future mandate.

The interinstitutional negotiations regarding the 2013 regulation were a long process and the main actors of the discussion defended harshly their positions. The resolution of the main controversies regarding the 2013 resolution happened thanks to the introduction of the common approach on decentralized agencies and the fact that the limited time allocated to the negotiations forced the European Parliament and the Council to ease their positions and find a consensus before the first reading.

As such, the Council, which had the more conservative posture in view of the Commission's proposal, gained the upper hand during the debates and managed to impose its views despite

²⁴⁹ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-Preparations for the Informal Dialogues with the European Parliament*, Brussels, 2012, 16872/12.

²⁵⁰ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-trialogues document*, Brussels, 2012, 11330/12.

²⁵¹ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-Preparations for the informal Dialogues with the European Parliament*, Brussels, 2012, 15994/12.

²⁵² Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-trialogues document*, Brussels, 2012, 11330/12.

²⁵³ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-Preparations for the informal Dialogues with the European Parliament*, Brussels, 2012, 15994/12.

²⁵⁴ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-Preparations for the Informal Dialogues with the European Parliament*, Brussels, 2012, 16872/12.

²⁵⁵ *Idem*.

the lack of common position in the Council regarding the duration of ENISA's mandate. Accordingly, the European Parliament tried to advocate for more substantial changes to the Commission's proposal regarding the 2013 regulation²⁵⁶. The ITRE Committee proposed a political control of the Parliament on the agency and tried to impose the idea of an executive board to the other principals but without much success.

If the 2013 regulation brought many changes on the functioning of ENISA, the period following the implementation of this regulation will, however, create the need to further evolutions in ENISA's functioning. As such, the 2013 European cyber strategy²⁵⁷ and the 2016 NIS directive²⁵⁸ will confirm the shift initiated by the 2013 regulation and ENISA will become an actor enshrined in the operationalization of the European NIS policy.

6.4 The 2018 regulation.

In regard of the 2018 regulation²⁵⁹, the interinstitutional debates are still going strong as the documents will only be presented to the voting during the plenary session of the European Parliament in September 2018²⁶⁰. Nevertheless, the Council and the European Parliament's ITRE Committee have managed to adopt firm positions on this text and some substantial amendments have been made.

The 2018 regulation originated from a long period of political negotiations. The 2016 NIS directive²⁶¹ had already spearheaded the negotiations. As such, a consensus on the main ideas of the 2018 regulation already existed between the principals before the beginning of the negotiations.

Consequently, if the 2013 regulation focused on the security aspects of ENISA's governance, the proposal for the 2018 regulation introduced key economic measures such as the long-awaited ICT certification which should effectively suppress the fragmentation of the European digital market. Nevertheless, a few peripheral controversies among the ITRE Committee and the Council appeared during the negotiations.

The peripheral issues were, in fact, legacies of the negotiations regarding the 2013 regulations. The beginning of the negotiations on the 2018 regulation witnessed some concessions made in favor of some of the propositions made by the European Parliament in 2013. As such, the European Parliament should enjoy a certain measure of political control over ENISA's executive director and the agency should have the possibility to sign administrative agreements

²⁵⁶ Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41.

²⁵⁷ Idem.

²⁵⁸ European Commission, *Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, Brussels, 2016, L 194/1.

²⁵⁹ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD).

²⁶⁰ Europarl, Legislative Observatory, [http://www.europarl.europa.eu/oeil-mobile/fiche-procedure/2017/0225\(COD\)](http://www.europarl.europa.eu/oeil-mobile/fiche-procedure/2017/0225(COD)), consulted on the 04/08/2018.

²⁶¹ European Commission, *Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, Brussels, 2016, L 194/1.

with third countries even though the Commission will need to give its agreement on these potential agreements²⁶².

Several operational tasks were also assigned to ENISA such as the obligation to produce a report in the aftermath of a cross-border cyber incident²⁶³. The essence of this kind of measures wasn't controversial but the Council, as usual, preferred to enshrine in the text that the consent of the concerned Member States were first necessary and that the inquiries should be limited by the imperatives dictated by national safety and the necessities of ongoing cyber-criminal investigations²⁶⁴.

The details concerning the establishment of the ICT goods and services' certification were, and still are, the most debated aspects of the 2018 regulation. If the principals agreed on the main aspects and procedures regarding the legal aspects of certification, some details were still unsatisfactory to the principals. The Council still has the most conservative opinion on this matter and its position is close to the original proposition of the Commission. Nevertheless, the Council managed to propose some amendments. These amendments concerned the national certification schemes important to the national safety of the Member States. Indeed, imposing Europe-wide certification schemes means that the Member States will not be able to produce national ICT schemes after the introduction of the 2018 regulation. This amendment insures that the Member States will remain autonomous in regard of national cybersecurity policies after the publication of the 2018 regulation. Conclusively, the position of the Council is determinate by the idea that ENISA's actions should complement the Member States' competences rather than effectively replace national cybersecurity policies.

The European Parliament is here more assertive on the subject of the process of certification. Once more, the ITRE Committee tries to advocate a far more precise framework for the certification process. In a note, the rapporteur even stated that the current conception of the certification process would lead to unsatisfactory schemes and that the 2018 regulation should allow the design of more specific schemes for the sake of efficiency²⁶⁵.

The other great priority of the ITRE Committee is to insure the involvement of stakeholder and Member States in the creation of the certification schemes²⁶⁶. As such, the initiative of a scheme's creation doesn't belong to ENISA but rather to the Commission and the European Cybersecurity Certification Group. This Group or the Commission must seize ENISA which will, in turn, propose a scheme that will be later implemented by the European authorities. The ITRE Committee proposed that institutions such as the permanent stakeholder group, internal

²⁶² European Commission, *Proposal for a Regulation of the European Parliament and the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2017, COM (2017) 477 final.

²⁶³ Idem.

²⁶⁴ Council of the European Union, *Proposal for a Regulation of the European Parliament and the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")-Examination of the Revised Version*, Brussels, 2018, 8209/18.

²⁶⁵ European Parliament, *Report-Proposal for a Regulation of the European Parliament and the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")* (COM(2017)0477-C8-0310/2017-2017/0225(COD)), Committee on Industry, Research and Energy, Rapporteur: Angelika Niebler, Brussels, 2018, 2017/0225(COD).

²⁶⁶ Idem.

to ENISA, could demand a new scheme to the Commission or the European Cybersecurity Certification Group which will launch the whole procedure²⁶⁷.

More interestingly, the ITRE Committee doesn't only propose measures reinforcing the production of schemes but also set terms for the limitation of the production of such documents. As such, the Committee advocates that the proposition of schemes should respond to several necessities set in the final version of the 2018 regulation²⁶⁸.

With the main area of debates described, it is apparent that the debates on the 2018 regulation are very different in nature to the interinstitutional negotiations regarding the making of the 2013 regulation. There is little frontal opposition between the Council and the Parliament but rather subjects that are still undermined and that future negotiations will have to give an answer to before the introduction of the text.

In conclusion, the balance of power between the principals stays sensibly the same during the negotiations regarding the 2018 regulation and the dialogues regarding the 2013 regulation. Knowingly, while the Council tends to advocate the maintaining of the Member States' autonomy regarding national security and seems to accept the spirit of the Commission's original text, the European Parliament tries to implement more ample reforms supporting the precision of ENISA's mandate and the involvement of the stakeholder in the functioning of the agency.

6.5 The balance of power between the European Parliament and the Council of the European Union in regards of ENISA's acts of delegation.

The proximity between the ambitions for ENISA, presented in the proposal of the 2004 regulation²⁶⁹, and the most recent version of the agency proposed by the 2018 regulation²⁷⁰ proved that the principals had a very clear vision for the future of the agency. Henceforth, the completion of the negotiations regarding the 2018 regulation could present the end of a cycle for ENISA as its role is now complete and any future changes can only be marginal modifications or, on the contrary, a drastic evolution of the agency or the NIS policy.

The analysis of the interinstitutional negotiations regarding the five regulations, being the acts of delegation of ENISA, revealed that the European Parliament and Council of the European Union had very clear priorities and objectives in regards of these debates. On the one hand, the European Parliament encouraged the involvement of a large array of industry and consumers related actors in ENISA's governance while specifying the role of the agency in the European cybersecurity landscape when, on the other hand, the Council managed to safeguard the autonomy of their respective national securities and gave ENISA a role as a complement of national NIS institutions rather than a competing level of power. Conclusively, the assumption

²⁶⁷ European Parliament, *Report-Proposal for a Regulation of the European Parliament and the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")* (COM(2017)0477-C8-0310/2017-2017/0225(COD)), Committee on Industry, Research and Energy, Rapporteur: Angelika Niebler, Brussels, 2018, 2017/0225(COD).

²⁶⁸ Idem.

²⁶⁹ Commission of the European Communities, *Proposal for a Regulation of the European Parliament and the Council Establishing the European Network and Information Security Agency*, Brussels, 2003, COM(2003) 63 final.

²⁷⁰ Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD).

stating that the Council tends to support intergovernmental interests while the European Parliament advocates a supranational agenda can here be accepted.

Nevertheless, the balance of power between the Parliament and the Council was clearly uneven in all of the different interinstitutional negotiations. The European Parliament tried to propose noticeable changes in the proposed regulations and to achieve some measure of political control on the management board and the executive director but without much success. On the contrary, the Council had a natural dominant position in the negotiation due to the sensitive issues touched by ENISA's mandate. As such, the disunity of the Council on several questions have forced the Commission to consider the opinions of the different Member States before proposing new regulations. It could be argued that the European Parliament proposed a great number of amendments to achieve some gains despite the already established status quo between the Commission and the Council.

Conclusion:

The purpose of this dissertation was to analyze the institutionalization process of a special European regulatory agency: the European Network and Information Security Agency. The specificity of ENISA is related to the policies that the agency has been charged to administer by the European legislator. The Network and Information Security policy, and at large any cybersecurity policies, is sensible for both the European and national interests due to their recent apparition in the political arena and its importance for national security of the different Member States.

The analysis conducted in this dissertation has proved that both the Member States and the European Commission had a clear idea of ENISA's role in the European cybersecurity landscape and how the agency should have evolved despite the initial reluctances of some of the Member States in the earliest stages of ENISA's history. It can be argued that the form and the missions of ENISA stayed true to this initial vision. Nevertheless, the recent operationalization of the tasks assigned to the agency has shown that the Member States may have lost a measure of control over ENISA's future as the agency gains more and more authority in a political field tainted by national security as well as economic harmonization. As such, the soon-to-be 2018 regulation²⁷¹ marks an end of cycle in the history of the evolution of ENISA's mandate as the original idea under the agency's creation will soon be implemented.

ENISA is the heart of the European Network and Information Security policy and accordingly is a convenient illustration of one of the key controversies regarding this political field: how can the European institutions articulate the imperatives of national safety, and all of the secrecy that it imposes, with the necessity of the harmonization of a fragmented European digital market?

The aim of this dissertation wasn't to give a clear response to this contradiction but rather to examine the effect of this controversy on the practical institutionalization of the most central actor of this policy field or, in other words, ENISA. As such, the research question *"How does intergovernmental and supranational interests have influenced the institutionalization of ENISA?"* was supposed to reflect these questions determining ENISA's mandate since its creation.

The choice was made to analyze the phenomenon from two points of view. The first point of view was supposed to examine the political debates on the documents defining ENISA's mandate: the different regulations founding the agency. The second perspective was internal to the agency in order to appreciate what kind of autonomy ENISA enjoyed in its action and what kind of institutions the Member States had created to insure that ENISA wouldn't deviate from its mandate. The two research hypotheses reflected these choices of analysis. The result of the analysis in regard of the research hypotheses will be discussed in the following parts.

²⁷¹ European Commission, *Proposal for a Regulation of the European Parliament and the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2017, COM (2017) 477 final.

- a. Findings of the research regarding the first research hypothesis: “The European Parliament and the Council of the European Union are the two principals of ENISA. The European Parliament tends to advocate for a supranational agenda while the Council of the European Union tends to defend an intergovernmental agenda”.

This first research hypothesis was the translation of the first ambition of this dissertation knowingly to understand the balance of power between the different European institutions in regard of ENISA’s mandate evolution and to understand the political motivations behind the creation of such an actor.

The opposition between the European Parliament and the Council is not an original concept as the scientific literature commonly associated the European Parliament with supranationalism and the Council with intergovernmentalism. As such, this first hypothesis was on questions widely discussed in the scientific community.

The research method was based on the analysis of the documents related to the debates surrounding the making of the different regulations in order to understand the themes, oppositions and recurring questions of these negotiations.

The findings of the research presented in this dissertation have validated this research hypothesis as these two actors have behaved accordingly with their alleged supranational and intergovernmental leanings.

The European Parliament advocated the reinforcement of ENISA’s role and legitimacy by precisising the scope and tasks of its mandate and by encouraging the different stakeholders of the industry to participate in the agency’s governance. More surprisingly, the European Parliament tried to reinforce the control mechanisms monitoring the agency’s action by, most notably, enforcing the political control of the Parliament over some of the key internal institutions of ENISA.

The Council defended the intergovernmental aspects of ENISA’s functioning by insuring that the autonomy of the Member States was respected and by asserting a strong national control over the management board of ENISA.

The relationship between the European Parliament and the Council during the interinstitutional negotiations was dominated by the Council as these institutions often had a position on the proposed regulation very close to the first proposal of the Commission. As such, the European Parliament tried to propose more innovative amendments but failed to influence the final documents repeatedly. This is most likely due to the fact that the Commission first consulted the different national delegations prior to the formal proposition due to the well-known reluctance of some of the Member States on ENISA’s evolution.

- b. Findings of the research regarding the second research hypothesis: “*The management board of ENISA is the main control mechanism set by the principals and defends intergovernmental interests*”.

The assumption of the importance of the management board over every other internal institution of a regulatory agency is also a recurring theme within the intellectual community. Conclusively, this hypothesis was built around the assumptions that, firstly, ENISA’s internal balance of power was faithful to the analysis of the scientific community, and secondly, as the national interests regarding cybersecurity policies were strong, it was more than likely that the management board defended the national interests of the Member States.

The research method was based on the analysis of the management board minutes and in the investigations of other internal institutions considered in the analysis of the intellectual community. As such, inquiries on the allocation of budgetary resources and the nomination of the executive director were also conducted.

This research hypothesis can also be validated, with some reserves, as the management board is indeed the most influential control mechanism within ENISA and tends to defend the national interests. However, these last statements must be nuanced. As such, if the intergovernmental interest tends to limit the reach of ENISA’s influence over the national cybersecurity policies, the management board has actively defended a certain idea of ENISA’s mandate and has insured that the agency’s actions stayed true to the mandate imposed by the European legislator. Conclusively, it can be argued that the management board has defended the functional aspects of ENISA’s mandate rather than limiting the agency’s governance within its mandate.

Bibliography.

1) Collective works:

- ADRIAENSEN, Johan, DELREUX, Tom, “Introduction. Use and Limitations of the Principal-Agent Model in Studying the European Union”, in ADRIAENSEN, Johan, DELREUX, Tom (Dir.), *The Principal Agent Model and the European Union*, Basingstoke, Palgrave Macmillan, 2017.
- RITTBERGER, Berthold, WONKA, Arndt, ‘EU agencies’ in RICHARDSON, Jeremy, MAZEY, Sonia (eds.), *European Union. Power and Policy-Making*, London, Routledge, 2015.

2) Monographs:

- CHRISTOU, George, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, Hampshire, Palgrave Macmillan, 2016.

3) Academic article:

- ALDRICH, Richard, HERRINGTON, Lewis, “The Future of Cyber-Resilience in an Age of Global Complexity”, *Political Studies Association*, 2013- vol.33 (4), 2013.
- ANDOURA, Sami, TIMMERMAN, Peter, “Governance of the EU: The Reform Debate on European Agencies Reignited”, *European Policy Institutes Network*, Working Paper n°19/October 2008, 2008.
- BACKMAN, Sarah, “Organizing National Cybersecurity Centers”, *Information & Security: An International Journal*, volume 32-2015, 2015.
- BARRINHA, André, CARRAPICO, Helena, “The EU as a Coherent (Cyber) Security Actor?”, *Journal of Common Market Studies*, JCMS 2017, UACES, 2017
- CHRISTOU, George, “The EU’s Approach to Cyber Security”, *EUSC EU-China Security Cooperation: Performance and Prospects*, Policy paper series, Autumn/Winter 2014, 2014.
- DUNN CAVELTY, Myriam, “A RESILIENT EUROPE FOR AN OPEN, SAFE AND SECURE CYBERSPACE”, *Swedish Institute of International Affairs*, Number 25 December 2013, 2013.
- E SILVA, Karine, « Europe’s Fragmented Approach towards Cybersecurity », *INTERNET POLICY REVIEW Journal on Internet Regulation*, volume 2 issue 4, 2013.
- HALL Peter, TAYLOR Rosemary, “Political Science and the Three Institutionalisms”, *Political Studies*, 44(4), 1996.
- JEPPESEN, Lene, TRANDAL, Jarle, “Images of Agency Governance in the European Union”, *West European Politics*, 31:3, 2008.
- KELEMEN, Daniel, MAJONE, Giandomenico, ‘Managing Europeanization: the European Agencies’ in Peterson J., Shackleton M. (eds.), *the Institutions of the European Union*. 3rd edition, Oxford, Oxford University Press, 2012.
- LORD, Christopher, *The European Parliament and the Legitimation of Agencification*, *Journal of European Public Policy*, 18:6, 2001.
- POLLACK, Mark, “Delegation, Agency, and Agenda Setting in the European Community”, *International Organization*, 51(1), 1997.

- RENARD, Thomas, “The Rise of cyber-diplomacy: the EU, its Strategic Partners and Cyber-Security”, *European Strategic partnership observatory*, Working Paper 7-June 2014, 2014.
- RITTBERGER, Berthold, WONKA, Arndt, “Introduction: Agency Governance in the European Union”, *Journal of European Public Policy*, 18:6, 2011.
- SLIWINSKI, Krzysztof Feliks, “Moving Beyond the European Union's Weakness as a Cybersecurity Agent”, *Contemporary Security Policy*, 35:3, 2014.
- THATCHER, Mark, *The Creation of European Regulatory Agencies and its Limits: a Comparative Analysis of European Delegation*, *Journal of European Public Policy*, 18:6, 2011.

4) Official publications:

a) European Commission

- European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Region: Network and Information Security; Proposal for a European Policy Approach*, Brussels, 2001, COM (2001) 298 final.
- Commission of the European Communities, *Proposal for a Regulation of the European Parliament and the Council Establishing the European Network and Information Security Agency*, Brussels, 2003, COM(2003) 63 final.
- Commission of the European Communities, *Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, 2007/0291 (COD).
- European Commission, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)*, Brussels, 2010, COM (2010) 521 final.
- European Commission, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions- Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyber space*, Brussels, 2013, JOIN (2013) 1 final.
- European Commission, *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, 2013, 2013/0027 (COD).
- European Commission, *Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, Brussels, 2016, L 194/1.
- European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT? THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, THE COMMITTEE OF REGIONS AND THE EUROPEAN INVESTMENT BANK: Investing in a Smart,*

Innovative, and Sustainable Industry, a Renewed EU Industrial Policy Strategy, Brussels, 2017, COM(2017) 479 final.

- European Commission, *Commission Staff Working Document: Assessment of the EU 2013 Cybersecurity Strategy*, Brussels, 2017, SWD (2017) 295 Final.
- European Commission, *Eurobarometer 464a: Europeans' Attitudes towards Cyber Security*, Brussels, 2017, 464a.
- European Commission, *PRESIDENT JEAN-CLAUDE JUNCKER'S State of the Union Address 2017*, Brussels, 2017, SPEECH/17/3165.
- European Commission, *Proposal for a Regulation of the European Parliament and the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2017, COM (2017) 477 final.
- European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2017, 2017/0225(COD).

b) Council of the European Union.

- Council of the European Union and the European Parliament, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency*, Brussels, 2004, L 77/1.
- Council of the European Union, *Communication from the Commission to the European Parliament and the Council on the evaluation of the European Network and Information Security Agency (ENISA)*, Brussels, 2007, 10340/07.
- Council of the European Union, *Preparation of the Transport/ Telecommunications and Energy Council of 12 and 13 June 2008: Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration-General Approach*, Brussels, 2008, 9768/08.
- Council of the European Union and the European Parliament, *Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 28 September Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2008, L 293/1.
- Council of the European Union and the European Parliament, *Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards its Duration*, Brussels, 2011, L 165/3.
- Council of the European Union, *Evaluations of the European Union Agencies-Endorsement of a Joint Statement and Common Approach*, Brussels, 2012, 11450/12.
- Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-Trialogues Document*, Brussel, 2012, 11330/12.

- Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-Preparations for the informal Trialogues with the European Parliament*, Brussels, 2012, 15994/12.
- Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)-Preparations for the Informal Trialogues with the European Parliament*, Brussels, 2012, 16872/12.
- Council of the European Union and the European Parliament, *Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004*, Brussels, 2013, L 165/41.
- Council of the European Union and the European Parliament, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")*, Brussels, 2018, 2017/0225 (COD).
- Council of the European Union, *Proposal for a Regulation of the European Parliament and the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act")-Examination of the Revised Version*, Brussels, 2018, 8209/18.

c) European Parliament.

- European Parliament, *Report on the Proposal of the European Parliament and the Council Establishing the European Network and Information Security Agency (COM (2003)63-C5-0058/2003-2003/0032(COD))*; Committee on Industry, External Trade, Research and Energy; Rapporteur: Reino Paasalinna, Brussels, 2003, A5-0353/2003 (FINAL)
- European Parliament, *Report-Proposal for a Regulation of the European Parliament and the Council on ENISA, the "EU Cybersecurity Agency", and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ("Cybersecurity Act") (COM(2017)0477-C8-0310/2017-2017/0225(COD))*, Committee on Industry, Research and Energy, Rapporteur: Angelika Niebler, Brussels, 2018, 2017/0225(COD).

d) ENISA.

- ENISA, *2005 Budget*, Heraklion, 2005, 2005 budget.
- ENISA, *2008 Budget*, Heraklion, 2008, 2008 budget.
- ENISA, *2016 Budget*, Heraklion, 2016, 2016 budget.
- ENISA, *Cyber Europe 2010-Evaluation Report*, Heraklion, 2011.
- ENISA, *List of ENISA Management Board Representatives and Alternates*, Heraklion, 2018, 24.05.2018.

- ENISA, *Minutes of the Second Meeting of the ENISA Management Board Held on the 14-15 September*, Heraklion, 2004, ENISA_MB/EL/JB/01_Draft.
- ENISA, *Minutes of the Fifth Meeting of the Management Board Held on 11 March in Centre Borschette, Brussels*, 2005, Brussels, Fifth meeting.
- ENISA, *Minutes of the 9th Management Board Meeting*, Heraklion, 2007, 9th meeting.
- ENISA, *Minutes of the 10th Management Board Meeting*, Heraklion, 2007, 10th meeting.
- ENISA, *Minutes of the 16th ENISA Management Board Meeting*, Heraklion, 2009, 16th meeting.
- ENISA, *Minutes of the Seventeenth ENISA Management Board Meeting*, Heraklion, 2006, 17th meeting.
- ENISA, *Minutes of the 19th ENISA Management Board Meeting*, Heraklion, 2011, 19th meeting.
- ENISA, *23rd ENISA Management Board Meeting*, Heraklion, 2013, MB/23/10.
- ENISA, *ENISA Management Board Extraordinary Meeting*, Athens, 2013, MB/2013-E/2.
- ENISA, *ENISA Management Board Extraordinary Meeting: 11 September 2014 Rome, Italy*, Heraklion, 2014, 24/09/2014.
- ENISA, *Draft Minutes of Extraordinary Meeting of the Management Board of ENISA Held on the 20 July 2017*, Brussels, 2017, 20/07/2017.
- e) European Court of Justice, Europol and the Official Journal of the European Union.
 - Official journal of the European Community, *Consolidated Versions of the Treaty on European Union and of the Treaty Establishing the European Community*, Brussels, 2002, C 325/1.
 - European Court of Justice, *Case C-217/04: United Kingdom of Great Britain and Northern Ireland against the European Parliament and the Council of the European Union*, Kirchberg, 2006, C-217/04.
 - Official Journal of the European Union, *Consolidated Version of the Treaty on the Functioning of the European Union*, Brussels, 2008, C 115/47.
 - EUROPOL, *Statement of Revenue and Expenditure of the European Police Office for the Financial Year 2016 — Amending Budget No 2*, La Haye, 2016, 2017/C 84/36.
- 5) Internet sources:
 - BOSCO, Francesca, *Assessing Europe's Cyber challenges*, internet policy review-journal on internet regulation, <https://policyreview.info/articles/news/assessing-europes-cyber-challenges/355>, consulted on 14/07/2017.
 - ENISA, Udo Helmbrecht-Curriculum Vitae, ENISA's website, <https://www.enisa.europa.eu/about-enisa/structure-organization/executive-director/udo-helmbrecht-cv/view>, consulted on the 12/07/2018.
 - Eurlex, Official Journal of the European Union, volume 47, 13 March 2004, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2004:077:TOC>, consulted on the 04/08/2018.

- Eurlex, Official Journal of the European Union, Volume 54, 24 June 2011, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2011:165:TOC>, consulted on the 04/08/2018.
- Eurlex, Official Journal of the European Union, Volume 56, 18 June 2013, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2013:165:TOC>, consulted on the 04/08/2018.
- Eurlex, Document 32013R0526, procedure, <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex:32013R0526>, consulted on the 04/08/2018.
- EUobserver, EU institutions hit by « major » cyber-attack ahead of summit, Euobserver, <https://euobserver.com/news/32049>, consulted on the 12/07/2018.
- European Commission, Digital Single Market: Policies: Cybersecurity, <https://ec.europa.eu/digital-single-market/en/cyber-security>, consulted on the 02/08/2018.
- European Commission, European Network and Information Security Agency Up and Running, site of the European Commission, <https://ec.europa.eu/digital-single-market/en/news/european-network-and-information-security-agency-and-running>, consulted on the 12/07/2018.
- European Union External Action website, Permanent Structured Cooperation (PESCO)-factsheet, https://eeas.europa.eu/headquarters/headquarters-homepage/34226/permanent-structured-cooperation-pesco-factsheet_en, consulted on 12/07/2018.
- Europol, About Europol, Europol website, <https://www.europol.europa.eu/about-europol>, consulted on the 12/07/2018.
- Europol, European Cybercrime Center-EC3, Europol website, <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>, consulted on the 12/07/2018.
- LEISTERER, Hannfried, New EU cyber security legislation: a Q & A with Andreas Schwab, internet policy review-journal on internet regulation, <https://policyreview.info/articles/news/new-eu-cyber-security-legislation-q-andreas-schwab/411>, consulted on 14/07/2017.
- The Guardian, Russia accused of Unleashing Cyberwar to Disable Estonia, the guardian, <https://www.theguardian.com/world/2007/may/17/topstories3.russia>, consulted on the 12/07/2018.