Universiteit Leiden

The cybersecurity landscape of the European Union

An institutional journey of EU cybersecurity cooperation from 2001 to 2018

MA International Relations, European Union Studies

Candidate : Max Cornelis Adriaan Balder
Student number: s1288601
Thesis supervisor: Dr. Vera Scepanovic
Word count: 15,535

The Cornfield by John Constable 1826. National Gallery London.

Contents

Introduction

What if we consider European Union cybersecurity as a landscape, just like the painting 'The Cornfield' from John Constable in 1826? The trees represent the member-states and the people and animals the EU institutions. The trees have existed before the people in the painting. The trees are old, have seen history envelop around them, there are different types of trees representing the different member-states each unique and still have the same basic needs like water and sun to grow (sharing characteristics). The trees will be there long after the humans and animals, the EU institutions, are gone. The trees provide oxygen for the humans to live just like, the member-states provide finances to the institutions and security to its people. The people look after the trees to prosper as well maintained trees are more likely to survive hardships like storms and they need to be protected from other trees that rival each other for the best place under the sun. The landscape painting portraits structure and unstructured at the same time which is typical for the complexity of cybersecurity.

Although the problem of integration is old, the domain of cyber is new, controversial and highly interesting. The classical understanding of sovereignty – meaning the monopoly over the legitimate use of force – is eroded as the digital domain does not pay attention 'to that territorial dimension of sovereignty which finds its expression in physical frontiers'.[1] States can no longer act alone in cyberspace as the economic and political system is imbedded in it. If they try to do so, by developing own rules in cyberspace or block of parts of the internet, they end up isolated from the rest of the world. Cybersecurity also involves the private and public sector. At the public level we have member-states that worry about how to achieve security, resulting in different policies. At the private level we see a booming but fragmented market in which goods and services have different levels of security that impacts the overall EU cybersecurity. At a macro level we see an EU that tries to develop coherence among the different preferences and approaches of member-states and finding its place among global cybersecurity actors.

The growing cybersecurity risks, attacks and threats create the impetus for data gathering, information processing and information sharing at the EU level to prepare and respond to these risks and dangers. This management requires a well-ordered and streamlined process to coordinate the actions of different stakeholders. Cybersecurity

[1] Marxsen, C., *Territorial Integrity in International Law* (Berlin, 2015) 5.

is a complex system that requires the coordinated efforts of these stakeholders in order to become resilient and robust. I posit coordination as the management of interdependent relationships that necessitates the exchange of information in order to align the actors' intentions, goals and actions.[2] The road towards increased coordination goes hand in hand with questions about how far such security integration must go. This is because (cyber) security integration contains questions about the future relationship between member-states and institutions: Who will spearhead this process? Who is responsible for the execution of policies? Currently, there are a number of actors that spearhead this development and it is paramount that they work together in order to promote coherent and stable coordination policies to reach sufficient EU wide cybersecurity.

The EU relationship with cybersecurity cooperation is complicated. This is because there are differences between cooperation in economic and security affairs that make successful cooperation within the EU a fragile topic. Economic cooperation is easier to achieve as its merits can be measured and countries in general gain from dismantling trade barriers. Security cooperation is a different issue as this is connected to high politics. The stakes in the area of high politics are perceived higher and it is much more difficult to assess the benefits of such cooperation as there are normally conflicting interests. Cybersecurity belongs to high politics because its interconnectivity and borderless nature means that one decision by one state has effects on the rest. As cybersecurity is complex and very well understood, a particular well-intentioned decision may be seen as hostile. This cooperation difficulty has to some extent to do with the balance of power and the security dilemma of the region. The security dilemma is the question of maintaining the balance of power by the prevention of a hegemon within the EU. Realism holds that the international system is anarchic and that states can only trust each other to a certain extent and will only seek cooperation if it is to their own interests. Cybersecurity is expensive to maintain and invest in which means that wealthier and bigger states can outduel smaller states and this unsettles the situation. Liberalism holds that institutions mitigate this anarchic system by preventing a single state to take a decision in regard to security without consulting it with other states and cooperation reduces costs and strengthen the abilities of states by the pooling resources.

[2] Chaudhary, T. & Jordan, J., 'Patchwork of confusion: the cybersecurity coordination problem', *Journal of Cybersecurity* (2018), Vol. 0 (0), 1-13.

The EU has cooperative mechanisms to mitigate this risk and promote multilateral cybersecurity cooperation. They are agencies, bodies and institutions that support the development of common policies: the Directorate General Connect on cybersecurity, European Defence Agency (EDA), the Permanent Structured Cooperation (PESCO), Europol (EC3), ENISA and the European Forum for Member-States (EFMS), the European Council, the European Commission and the European Court of Justice (ECJ). I am interested the most in Europol(EC3), ENISA and the EFMS because these bodies focus on cybersecurity and I exempt the EDA as cyberdefence is outside the scope of this thesis. When these agencies were created, they had to earn their place within the institutional framework. This is not easy when they operate in the area that touches upon the issue of sovereignty which is jealously guarded by the member-states. Europol/EC3 facilitates the coordination of national Law Enforcement Agencies (LEA) against cybercrime by analysing and sharing information. Cybercrime is a major concern for the EU and the fight against it is one of the pillars of the *Cybersecurity Strategy*. EFMS is an intergovernmental platform for member-states to develop joined policies and exchange best practices and information. Its purpose is to align policies, to hammer out as much agreement as possible and support formal decision-making. ENISA coordinates national cybersecurity strategies (NCSS) to ensure policies converge and provides knowledge and expertise to member-states and EU institutions. It has a coordination responsibility in the event of cyberattacks. Its major responsibility is to ensure that member-states implement the policies necessary to meet the legal and regulatory obligations of the Network and Information Security (NIS) Directives.

These agencies did not get these competences in one go. Rather, as my thesis will show, this was a long incremental process of 18 years. Some did not start as agencies but as bodies outside the institutional framework and were later adopted as formal EU agencies. This process can be dubbed as institutionalisation. This concept connects the existence of bodies called institutions with the alteration of spheres of influences within an institutional setup. Member-states and institutions start each with a set of competences, but as time passes by, it can occur that either one of them gains more responsibilities from the other and thus gain more weight within the institutional setup to generate specific norms and shared believes of understanding about specific policy issues (e.g. cooperation) which are taken over by the recipient.

The aim of my thesis is to understand how these three institutions became more robust and gained more competences within the institutional setup of the EU. Of these three I use ENISA as a case study to clarify how far institutionalisation can go. Why?

Because since its creation in 2004, it has developed exceptionally well up until the recent Cybersecurity Act in December 2018. The fact that this Act was passed within three months indicate the importance cybersecurity on the political agenda. My main research question to understand the institutionalisation process is: *How did the EU cybersecurity institutionalisation develop between 2001 and 2018?* I look for evidence within the body of *EU Communique* – Directives, Council Conclusions, publications and reports – to understand how and possibly why these institutions became more influential within the 18 year timeframe.

I need to distinguish what I describe as evidence of institutionalisation in order to answer the research question. Therefor I construct an analytical framework based on the work of Michael Smith on institutionalised cooperation, to look for evidence of institutionalisation:

(1) Competence stretching

(2) Feedback loop

(3) Entrepreneurship of the European Commission

My framework draws upon the 'new institutionalism' literature (which involves Rational Choice Institutionalism, Historical Institutionalism and Sociological Institutionalism) in the attempt to provide a coherent way to understand cybersecurity institutionalisation. Neoinstitutionalism holds that institutions matter for a number of reasons and my own argumentation in this thesis puts me closer to sociological institutionalism because the institutions at the very least provide memory about previous decisions and they possess resources like knowledge and expertise that allow them to have sufficient weight with member-states.

This thesis is divided in four chapters, each designed to contribute to answering the research question. The first chapter will show how new institutionalism in general and sociological institutionalism in particular offer tools for understanding evolution of deeper cooperation in cybersecurity matters in the EU. In the second chapter I discuss in more detail my analytical framework for the analysis of the chosen agencies. My third chapter introduces the three cybersecurity institutions and gives an understanding what they do and how they relate to each other. My fourth and final chapter is the analytical heart of this thesis. In it I use empirical evidence from EU documents to explain why ENISA has developed in the most advanced cybersecurity institutions to date and where the impulse for this development has come from. I finish with a conclusion about this study and provide new research suggestions.

Chapter 1. Theory

This chapter will elaborate on the theoretical foundations on which this thesis is built. It starts with an introduction on institutionalism in which different theoretical streams of new institutionalism are confronted. It also discusses how they have been used to analyse the process of Europeanisation.

1.1 Institutionalism – an introduction

In order to understand the European integration process of cybersecurity cooperation, it is important to understand the institutional dynamics behind it. In order to do so, neoinstitutionalism is used to understand the 'institutionalisation' of cybersecurity. Neoinstitutionalism is a powerful theory that explains the Europeanisation of policies and proved its value in socio-economic and security studies.[3]

The starting point of neoinstitutionalism is that institutions matter. Neoinstitutionalism takes institutions as the unit of analysis and perceives them as having sufficient political power and weight to affect actions and outcomes. They are considered to be an autonomous force in politics.[4] This thesis adopts the definition of institutions developed by Hall and considers institutions as formal rules, standard operating procedures, formal institutions and customary practices which influence actor behaviour and policy choice.[5] It does so since Hall's work is considered an authority in the field of institutionalism and facilitates the understanding of a single definition of institution that will be used throughout the thesis.

The name new institutionalism implies the existence of a former institutionalism that is called 'old institutionalism' which saw institutions as material structures like constitutions, parliaments and bureaucracies. In other words, institutions referred to the state or government.[6] Lecours traditional institutionalism focused primarily on the analysis of the level of success of formal institutions and gave recommendations for future institutions, but did not explicitly theorize about institutions but remained largely descriptive and normative.[7] At the core of this old institutionalism was the belief

[3] Robert, L., 'Europeanization and Political Parties: Towards a Framework for Analysis', *Journal of Common Market Studies* (2004), Vol. 52 (4), 577.
[4] Violakis, P., *Europeanisation and the Transformation of EU Security Policy Post-Cold War Developments in the Common Security and Defence Policy* (Routledge, 2018) 36.
[5] Hall, P., 'Political Science and the Three New Institutionalisms', *Political Studies* (1996), Vol. 44 (5), 937.
[6] Lecours, A., 'New Institutionalism: Issues and Questions' in: Lecours, A. (ed) *New Institutionalism: Theory and Analysis* (University of Toronto Press, 2005) 6.
[7] Lecours, 'Issues and Questions' 10.

that if there was a theory about institutions, it was 'legal and constitutional' and did not explain the behavioural assumptions that would be more present in new institutionalism.[8]

Neoinstitutionalism on the other hand is an approach that combines the traditional thinking of institutionalism which focuses on the formal institutional rules and structures, with the behavioural school of thought which examines the actions of political actors in order to explain the process of political outcomes of institutions.[9] This theory explores how institutional rules, structures, norms and cultures influence political behaviour by constraining the choices, room for manoeuvre and political outcomes. Institutionalisation is then understood as a mechanism by which norms and shared interests and behaviour are created and developed.[10] (Cybersecurity) institutions develop because they have an added-value to member-states and the EU. They can develop norms and values which gives them legitimacy to member-states because what they do is considered legitimate. Indeed, institutions are powerful because they can shape the interests and preferences of their members by providing knowledge that facilitate norms building and harmonisation.[11] In addition, institutions are influential as they offer participants a platform for meetings on a *regular* basis. As the organisation of meetings, conferences etc. uses time, resources and locations, the institutions are perfectly suited to facilitate these. The enormous institutional buildings in Brussels indicate the ability to hosts large meetings and conferences. The regularity of meeting implies the continuity of cooperation between actors as it is easier to use existing platforms for exchanging thoughts and information which reduces costs. In order to understand cybersecurity institutionalisation it is required to consider how norms and behaviour change over time. Change is a constant feature for most institutions and it is therefore not only important to define what an institution is, but rather what an institution is becoming. Fundamentally, institutionalisation means change.[12]

Institutionalisation is connected to the thinking of 'Europeanisation' whereby the EU political and economic dynamics affect the reorientation of the direction and shape of national politics to such a degree that they become part of the organisational logic

[8] Hall, P., 'Politics as a process structured in space and time' in: Fioretos O (ed.), *The Oxford Handbook of Historical Institutionalism* (Oxford University Press, 2016) 33.
[9] Smith, *Europe's Foreign and Security Policy* 20.
[10] Ibidem, 25.
[11] Ibidem, 27
[12] Ibidem, 34.

of the EU.[13] The study of Olsen has shown that Europeanisation cannot be defined in a single definition. Instead he argues that Europeanisation consists of a number of processes of construction, diffusion and institutionalisation of formal and informal rules, policy convergence, shared beliefs and norms and 'ways of doing'. They are first defined at EU level and then incorporated in the logic of discourse and political structures at the national level. Each of these models reflect the many 'faces' of Europeanisation.[14] This means that Europeanisation must not be interpreted as a linear top-down notion, but instead as an interactive process. These different models explain why the explanation of Europeanisation varies depending on the issue and policy area and why a lot of research has therefor focused on the processes through which different forms of Europeanisation are achieved. My thesis tries to contribute to the debate on Europeanisation by the focus of this topic via the lens of cybersecurity cooperation. This offers added insights in how Europeanisation works in different policy fields.

These different models allows me to define Europeanisation in two ways: (1) there is the notion of Europeanisation as policy convergence, where the cognitive and normative policy frames of national policy are gradually redefined along European lines, where member-states adopt similar ideas, norms and standards of behaviour. This definition shows the socialisation effect of the EU. The institutions are the channels through which this socialisation occurs as the EU provide the frames, norms and terms of reference. Then there is Europeanisation as a transfer of responsibility for enforcement of all this to the European level (e.g. Customs Union).

Europeanisation sets a link between the evolution of EU rules and the 'adaptational pressure' exerted on national levels when the domestic institutional settings differ.[15] According to Borzel and Risse this pressure has to do with the nature of the EU in which there must be a constant degree of 'misfit' or incompatibility between EU policies, processes and institutions on the one hand and national policies, processes and institutions on the other.[16] It is also about the (in)congruence between EU policies and the willingness of national policymakers to accept.[17] When EU policies have a similarity to those at the domestic level, the pressure to reform is expected to be much

[13] Ladrech, R., 'Europeanization of Domestic Politics and Institutions: The Case of France', *Journal of Common Market Studies* (1994), Vol. 32(1), 69.
[14] Olsen, J. 'The Many Faces of Europeanization', *Journal of Common Market Studies* (2002), Vol.40(5) 923.
[15] Lavenex, S., 'A governance perspective on the European Neighbourhood policy: Integration beyond conditionality?', *Journal of European Public Policy* (2008), Vol. 15(6) 941.
[16] Borzel, T. & Risse, T., 'Conceptualising the Domestic Impact of Europe' in: Featherstone, K., (ed.), *The Politics of Europeanisation* (Oxford University Press, 2003) 28.
[17] Caporaso, P., *Theorizing Europeanisation* (Cambridge, 2008) 29.

lower. Reforms in the field of economics generate enormous domestic pressure since they tear into the existing institutions and established privileges of socio-economics groups. Cybersecurity on the other hand is a relatively new field and the institutions and preferences are not so strongly formed yet. Thus we can expect pressure to reform to be lower. The cybersecurity communities involved are already transnational and share similar organisational culture so Europeanisation of politics should be much easier. Member-states who do not have a successful cybersecurity strategies in place are more susceptible to cybersecurity institutions (as they offer the know-how) which allow for policy convergence between domestic and European level. Member-states who already possess well-functioning cybersecurity strategies tend to be less susceptible and tend to question institutional interference.[18] However, the opposite is true as well. New institutions do not have a proven track record to legitimise their creation and influence and they must constantly adjust their perspective within the institutional development of the EU. They also need to work with other institutions who might have areas of jurisdiction taken away by the new one adding to institutional ambiguity.

While all institutionalist theories accept the importance of pre-existing institutions for development of further cooperation, they differ in their view of the mechanisms through which such cooperation happens. My next section will discuss the different institutionalism.

[18] Schimdt. V., 'Democratic Legitimacy in a Regional State?', *Journal of Common Market Studies* (2004), Vol. 42 (4) 331-355.

1.2 Three different institutionalisms

There are three approaches within institutionalism that offer an explanation to cybersecurity institutionalisation. They are Historical Institutionalism, Rational Choice Institutionalism and Sociological Institutionalism.

1.2.1 Rational Choice Institutionalism

Rational Choice Institutionalism (RCI) tries to understand how institutions limit or provide opportunities to strategic actors.[19] According to RCI players of the political game have a particular set of preferences they wish to attain, behave accordingly and do so in a strategic manner that involves careful calculation.[20] These actors do so within the context of the rules and incentives that characterise institutions. This perspective allows us to understand institutions as the set of formal and informal rules each actor should adhere to in order to play the political game.[21] RCI connects goal attainment with the viability of institutions. The functional logic behind this is that if goals are better achieved via the institution, that institution is granted more responsibilities to support the goal attainment. This suggests that RCI explains competence building of cybersecurity institutions because member-states' goals cannot be sufficiently achieved at the national level but can be at the EU level. This has to do with the issue of collective action dilemma and transaction costs.

The concept of collective action dilemma is used by RCI to analyse policy. This dilemma arises from the division of authority in which decisions by one actor in a specific functional area impact other actors and other policy fields.[22] Conflicting interests among actors are seen as the single cause for this dilemma as, although these actors want to achieve certain collective goals, their own interests may hamper efficient cooperation. Actors tend to develop bilateral cybersecurity issues as the issue of trust is signification for cooperation: security cooperation is based on trusted relationship, if that is breached diplomatic relations may break down. The challenge of cybersecurity institutions is to generate a collective acceptable balance where on the one hand the

[19] Weingast, B. & Marshall, W., 'The Industrial Organization of Congress', *Journal of Political Economy* (1988), Vol. 96(1) 134-135.
[20] Hall, 'Political Science' 12; Shepsle, K., & Weingast, B., 'The institutional foundations of Committee Power', *American Political Science Review* (1987), Vol. 81(1) 89.
[21] Weingast, B., 'Rational-Choice Institutionalism' in: Katznelson, I., *Political Science: The State of the Discipline* (New York, 2002) 666.
[22] Feiock, R., 'The Institutional Collective Action Framework', *Policy Studies Journal* (2013) Vol. 41(3), 397.

collective goal is achieved and on the other hand the preferences of the individual actors are taken into account. The EU is unique insofar that the member-states and the EU try to develop a balance of mutual benefit. The challenge is to not upset the balance too much insofar that a different outcome would make one actor better off than others. As these actors move around in a realist world where trust is a determinant for cooperation and with it a particular outcome, institutional structures can reduce uncertainty and potential risks associated with action and inaction.[23] To this regard, Institutions are then seen as equilibriums of the strategic interactions between these rational actors. The more institutions contribute to the resolution of collective action dilemmas and to add gains to member-states, the more robust it will become.[24] The RCI method allows us to understand that the existence, emergence and survival of institutions are due to the fact that they are beneficial to the actors involved.

RCI suggests that institutional change occurs when the institution under inquiry is dysfunctional or does not generate optimum results. The institutional equilibrium is thus the norm when actors try to maximise their goals within the institutional context and the institution is held constant. This perspective is reinforced by RCI that views institutional change as a consequence made by the strategic decisions of actors. Member-states remodel a cybersecurity institution when it is considered as ill-equipped to contribute to collective outcomes (information exchange). This entails that rules and practices need to change in order to generate a new equilibrium.[25] Institutional change is thus a modification as member-states realise that the benefit of change outweighs the costs and move towards a new equilibrium. The transaction costs of change refers to the costs of changing and operating it and is connected with the costs to learn how to operate within the new environment.[26] Both the member-state and the institution have to adjust to their new relationship when mandates are amended, new policies are introduced or new institutions emerge.

[23] Feiock, 'The Institutional', 400.
[24] Ibidem, 411.
[25] Scheinder, G. & Ershova, A., 'Rational Choice Institutionalism and European Integration', *Oxford Research Encyclopedia of Politics* (Oxford University Press, 2018) 3.
[26] Lowndes, V., 'The Institutional Approach' in: Marsh, D. (ed.), *Theory and Methods in Political Science* (Palgrave, 2002) 66.

1.2.2 Historical Institutionalism

Historical Institutionalism (HI) defines institutions as organizational structures in which it has embedded formal and informal procedures, routines, norms and conventions.[27] Institutions provide strategically-useful information that allows them to shape the interests and preferences of actors.[28] Central to HI is the notion of a historical based analysis in order to reveal why actors reiterate certain goals and preferences over others.

According to North, institutional change shapes the way societies evolve through time and is thus key to understand historical change.[29] Continuity is a central component in HI and an apparent change actually hides underlying continuity. Historical institutionalists believe that the way institutions behave has a contextual cause in which a given situation is inherited from the past and that it is normally the historical landscape that changes whereby the institutions are a persistent feature.[30] This is connected to the concept of path dependency. This is a crucial element to HI since this entails a dynamic process of self-reinforcing.[31] This means that when a given institution is formed or policy initiated, positive feedback (based on initial policy choices) reinforces that particular path, hence we talk about 'self-reinforcing historical paths'. Reforms within EU cybersecurity policies are then understood as a continuation of the chosen path. The central elements of HI allow for the argumentation that the development of cybersecurity policy and institutions enable the EU to reinforce its path of institutionalized cooperation.

HI suggests that the once a particular policy is initiated, institutional change is actually evidence of a continuous process. When institutional change does occur, HI argues that this is the result of unintended consequences that form 'critical junctures' up to a particular 'branching point' where the institution embarks on a new path. Margaret Levi uses the metaphor of a tree instead of a path to explain path dependence. As all institutions or actors start from the same conditions – or tree trunk – there are various branches. It is possible to climb from one branch to a different branch, yet the

[27] Hall, 'Political Science' 938.
[28] Olsen, J. & March, J., *Rediscovering Institutions: the organizational basis of Politics* (Free Press, 1989) 23.
[29] North, D., *Institutions, Institutional Change and Economic Performance* (Cambridge University Press, 1990) 3.
[30] Lowndes, 'The Institutional Approach'; Krasner, S., 'Sovereignty: An Institutional Perspective,' *Comparative Political Studies* (1988) Vol 21(1) 66–94; Downing, M., *The Military Revolution and Political Change: Origins of Democracy and Autocracy in Early Modern Europe* (Princeton, 1992); Pierson, P., 'Increasing Returns, Path Dependence and the Study of Politics', *The American Political Review* (2000) Vol. 94 (2) 251-267.
[31] Hall, 'Political Science' 951.

branch on which you begin your climb you tend to stick with it.[32] HI presumes that whenever an institution embarks on path / branch it is difficult to alter or reverse this trajectory as positive feedback (strong branches) provide the scenario of self-enforcing. Consequently the situation exists in which the sequence of institutional choices over time increases the payoff for certain choices in the future as North claims.[33] Simultaneously, institutional change occurs when this feedback and self-reinforcing process stops working – or the branch breaks down – forcing the political actor – climber – to choose a new path. Institutional change is therefor rather incremental than radical as new institutions are created on top of existing stable institutions (the same tree trunk) and old institutions are remodelled for new purposes.[34]

What does HI expect to happen in the balance of power between institutions and political actors when change occurs? How will the institutional configuration looks like after this change? According to the principles of HI, institutions are seen as tools that provide political actors with relevant information (e.g. historical experiences) about the behaviour of others, mechanisms for agreements (e.g. council meetings) and penalties for defection (e.g. fines).[35] This means that after the configuration the possibility that institutions gained more competences is more likely. A consequence is a shift in the balance of influence between the actors involved (member-states and institutions). For the member-states a positive development is their accessibility to more information and mechanisms for agreements. New bodies, agencies or fora are then utilised as new platforms for operational, strategic and political cooperation. With the transfer of competences institutions shape member-states' preferences, their corresponding strategies and goals because they offer more optimal information to member-states to make wise necessary decisions then when member-states simply use bilateral agreements. Following this approach, institutions are seen as a moral guidance towards actors and give a certain rulebook for analysis and action. This is not always seen as a positive development. HI can also view institutional development in negative terms. If institutions embark on a new path, this is because the member-states lacked the capacity to control them or because European organizations like the Commission did not

[32] Levi, M., 'A Model, a Method, and a Map: Rational Choice in Comparative and Historical Analysis' in: Lichbach, M. (ed.), *Comparative Politics: Rationality, Culture and Structure* (Cambridge, 1997) 28.
[33] North, 'Institutions' 95.
[34] Thelen, K., 'Historical Institutionalism and Comparative Politics', *Annual Review of Political Science* (1999) Vol. 2 (3) 377.
[35] Hall, P., 'Historical Institutionalism in Rationalist and Sociological Perspective' in: Mahoney, J. (ed.), *Explaining Institutional Change – Ambiguity, Agency and Power* (Cambridge, 2010) 204-223.

possess enough autonomy to control change.[36] When the EU takes on new issues – embarking on a new path – it tends to be reluctant to give it back and sticks with the chosen course unless critical junctures or catastrophic events come to force a change.

1.2.3 Sociological Institutionalism

What distinguishes Social Institutionalism (SI) from the other approaches is that it puts an emphasis on the cognitive instead of the historic (HI) or strategic (RCI) aspect of institutions. SI defines institutions much broader which includes cognitive scripts, moral templates and symbol systems as these provide the 'frames of meaning' that guides and constrain human behaviour.[37]

From the perspective of SI, institutions develop because they add legitimacy to a particular course of action. Actors comply with institutions not because of rational cost-benefit calculations but because they have a shared understanding of what is legitimate.[38] This 'logic of appropriateness' then either improves or degrades certain actions.[39] Institutional change follows the same explanation as institutional formation, which occurs when a particular course of action does not increase legitimacy. The theory's strength derives from its assumption that actors do not act solely on rational grounds. Cognitive abilities of decision-makers are limited due to bounded rationality by the overflow of information. Institutions are then considered to be 'coping mechanisms' instead of utility-maximizing one (RCI approach) to go beyond the cognitive limits of human capability to process information.[40] To that extent institutions are knowledge powerhouses filled with experts who belong to an epistemic community. Institutions develop reports on subject matters and because they are the experts, the reports carry weight. This lead to the assumption that member-states rely on institutions that act as standard cooperating procedures to facilitate a shared understanding of what is appropriate within cybersecurity cooperation and thereby structure and coordinate action.

---

[36] Smith, *Europe's Foreign and Security Policy* 32.
[37] DiMaggio, P. & Powell, W., *The New Institutionalism in Organizational Analysis* (The University of Chicago Press, 1991) 28.
[38] Hall, P., 'Historical Institutionalism' 211.
[39] Lewis, J., 'The Janus Face of Brussels: Socialisation and every day decision making in the European Union, *International Organisation* (2005) Vol. 59(4) 951.
[40] Rasmussen, G., 'Frames, agency and institutional change: the case of benchmarking in Danish construction', *Construction Management and Economics* (2017), Vol. 35(6) 312.

SI suggests that policies are dealt with within the institutional set-up when actors deem it is the right thing to do. This has a lot to do with how issues are framed and is a central concept within SI. Framing entails that certain issues are constructed in such a manner as being significant enough to be dealt with at a particular political level and with a certain political mechanism.[41] Next to this, framing also constitute the linkage between a problem and a solution.[42] Due to the limitations of actors to process information, framing can determine policy choices and is a powerful instrument to use 'in order for certain policies to be placed on the political agenda'.[43] For the EU this does not only include the available policy options, but also to construct the appropriateness of the EU as the suitable level of governance to tackle the issues.[44] Certain international incidents – 2007 cyberattacks on Estonia – prompt the EU to place itself as the suitable player to articulate cybersecurity policies. When we consider the above, SI allows for the argumentation that cooperation occurs because either the EU is successful in framing the problem of cyber *insecurity* to be significant enough that it can be tackled efficiently (solution) via its institutions or institutions are coping mechanisms to deal with the input of data. Obstacles – insufficient information sharing capabilities, jurisdictional boundaries, disparities in technical capabilities – for efficient cooperation continue to exists and can only be solved when the EU's solutions are accepted. It is interesting to see that reviews, reports, proposals and plans from the Commission and the cybersecurity institutions always predict the answer for more cybersecurity to be more cooperation at the European level. This pushes institutions and member-states to cooperate together as the efficiency of their cooperation is the benchmark to legitimize their chosen course of action. The EU institutional set-up requires supra-national institutions (e.g. EP) to work with intergovernmental institutions (the Council) in order to reach decisions. The EP needs its co-legislator, the Council, to approve and adopt laws.

[41] Rasmussen, 'Frames, agency and institutional change' 311.
[42] Princen, S., 'Agenda-setting in the European Union: a theoretical exploration and agenda for research', *Journal of European Public Policy* (2007), Vol. 14(1) 24.
[43] Princen, 'Agenda-setting', 20.
[44] Ibidem, 30-33.

Chapter 2. Towards a framework for studying institutionalization

The previous chapter addressed the different types of institutionalism that can explain the institutionalisation of cybersecurity. In order to analyse the level of institutionalisation I need to construct a framework in order to do so. Based on the previous chapter I distinguish three mechanisms of institutionalization. Throughout the thesis I use them to highlight the level of institutionalization between 2001 and 2018.

(1) *Competence stretching*. It is possible for states to cooperate and develop norms without an explicit agreement. However, it is more likely that they make public announcements that they create organizations to facilitate their cooperation. Once member-states agree to establish an institution to reach common goals, there must be some sort of oversight to ensure objectives are reached and member-states fulfill their obligations. An institution becomes stronger when a clearer articulation of the functional goals and norms is visible in EU policies. Amendments in policies, new mandates or references to the institution in strategies illustrate competence stretching of the institution. This can be measured in the *EU Communique*. On the other hand, if we see a decline in articulation this can illustrate that the balance between the member-states and the institution shifts. The institutional services are used less and member-states find other ways to cooperate (to find a new equilibrium). The result is an institution that is subject to change if it wishes to remain beneficial towards the member-states.

(2) *Feedback loop.* When an institution functions it receives feedback about its performance. This feedback can develop into a loop where the institutional positioning as a hub for expertise and cooperation are acknowledged and the institution can expand its competences. This reflects the 'logic' of the institutional system as being the right way to do business and reinforces the path of institutionalized cooperation.

(3) *Entrepreneurship of the European Commission.* The Commission's interaction with all member-states allows it to present an issue as a priority on the political agenda and increase EU's policy streams. These policy streams consists of various solutions to issues that member-states care about: single market, cyberattacks and vulnerable infrastructure. The Commission can frame the discourse and problems to influence the interpretation of the problem and predetermine

possible answers. The Commission puts an emphasis on its institutions as knowledge hubs in order to promote the legitimacy of its policies. They also allow for a channel of influence for member-states: room for discussion and debate and access to expertise.

Chapter 3. The EU cybersecurity institutions

I use three cybersecurity institutions as part of my analysis to show how the EU cybersecurity institutionalization developed. They are: EC3[45], ENISA and the EFMS. They are the channels through which the EU provide the terms of reference, norms building and cooperation. How does the analytical framework and the theory chapter understand the development of these institutions?

Europol – the High-Tech Crime Centre and European Cybersecurity Centre

Prior to the establishment of Europol in 1999, the tackling of cybercrime was carried out on a bilateral basis.[46] This proved to be difficult with cybercrime as it affected multiple member-states with the need to involve more Law Enforcement Agencies (LEA). If there was no agreement between countries their LEAs could not cooperate and exchange information which created a limited perspective on criminal networks. When Rational Choice Theory (RCI) is applied to Europol we can understand the creation of this institution as a rational choice from member-state to address cross-border criminality by enhancing their police cooperation.[47] The creation of an independent actor would not upset the balance of power between rational member-states because it is accountable to the Commission and to maintain some control and authority: Europol's mandate was limited to information sharing competences and not to 'kick doors down'.[48] This means that Europol does not have execute judicial authority but acts as a central nexus for criminal intelligence with its information processing capacity. In 2002 the 'High-Tech Crime Centre' (HTCC) was established within Europol to focus on online criminal activities which reflected the growing need for a centralized multidisciplinary response to cybercrime.[49] It also reflects the 'competence stretching' mechanism as the need to address cybercrime was to extend the competence of an institution the creation of an extra body within it. In other words: Europol would not only house offline crime expertise, but also online crime expertise. Via the HTCC, the EU developed another avenue for information-sharing and cooperation to secure European cyberspace and free it from cybercrime.[50] In 2013 the

[45] Until 2013 it was called the 'High-Tech Crime Centre' (HTCC).
[46] Europol, *Annual Report 2013* 3.
[47] Europol, *Annual Review 2010* 4.
[48] Dewar, R., *Cybersecurity in the European Union: an historical institutionalist analysis of a 21st century security concern* (PhD dissertation, 2017) 152.
[49] Europol, *Annual Review 2012* 38.
[50] European Commission (2004) 401 3.

HTCC was renamed into the European Cybercrime Centre (EC3) signaling the importance of a central European node for criminal intelligence related to online crime. This evolutionary path of Europol, the HTCC and EC3 strongly suggests that Historical Institutionalism (HI) and Sociological Institutionalism (SI) are at work here. The path dependency of this institution is understood with the 'feedback loop' mechanism. To tackle crime, member-states needed an institution to tackle transnational crime as they were unable to cope with this problem by themselves. The creation of Europol/HTCC/EC3 is thus a 'coping mechanism' as SI explains. When cybercrime developed, the positive feedback from member-states about Europol's expertise reinforces the chosen path of institutionalize police cooperation. The HTCC and EC3 are built consecutively to foster cooperation on cybercrime and their policy output receives sufficient positive feedback to stretch their competences.

These institutions were able to develop thanks to the effort of the Commission. My third mechanism puts the Commission as an entrepreneur that can frame certain solutions as being the best possible solution towards problems. When the 2011 *Directive on Child pornography* and the 2013 *Directive on attacks against information systems* were adopted, it positioned the EC3 as the 'European cybercrime information focal point' and it would pool European cybercrime expertise together.[51] This could mean that the Commission was very effective with these two Directive to frame its institutions as being the best possible policy solution.

ENISA – the European Network and Information Security Agency

In 2004 the European Network and Information Security Agency (ENISA) was established to enhance EU and member-state capabilities and prevent Network and Information Security (NIS) problems.[52] Its mission is to achieve a high level of NIS and develop a cybersecurity culture within the EU. It does this by being the centre of expertise for member-states, shares experiences and best practice, publishes guidelines for member-states and helps them to develop national cybersecurity strategies (NCSS).[53]

The theory of SI and HI explain the evolution of ENISA very clearly. In order to deal with the complexity of cybersecurity, this institution is created to act as a coping

[51] Directive 2013/40/EU, *On attacks against information systems and replacing Council Framework Decision 2005/222/JHA*; Directive 2011/92/EU, *On combating the sexual abuse and sexual exploitation of children and child pornography.*
[52] Council Regulation 460/2004, *Establishing the European Network and Information Security Agency.*
[53] Ibidem, 2.

mechanism. In order to achieve its mission, ENISA wants to be the centre of expertise in order to attract the attention of member-states to use its services. When member-states acknowledge the expertise of ENISA, the logic would be to refrain from building different mechanisms but instead use ENISA because it is the appropriate thing to do precisely because it is the centre of expertise.

The Commission supported ENISA with the *European Union Cybersecurity Strategy* (EUCS) in 2013. This policy obligated member-states to adopt their own NCSS and positioned ENISA as the actor to align national policies with EU policies and thus generates a more coherent and European coherence style based on a holistic approach and actor cooperation. The EUCS limited the scope of ENISA: it does not focus on cyberdefence but on cybercrime with business and public policy solutions. It develops ICT certification schemes for goods and services to ensure minimum security and it has operational capabilities with adoption of the *Cybersecurity Act* adopted in November 2018. Its normative impact on member-states is not to be underestimated as it fosters a cybersecurity culture throughout the EU.[54] Its added value lies in the ability to provide an independent platform to asses cybersecurity problems and offer solutions.[55]

In terms of cooperation ENISA, is at the heart of the EU cybersecurity landscape. It facilitates and coordinates responses to cybersecurity incidents by staging annual cybersecurity exercises of which the first one took place in 2012. 'Cyber Europe' highlighted crucial aspects of cooperative responses like the need to build capabilities, share information between actors, to raise awareness and give more training workshops.[56] The original mandate of ENISA states nothing about hosting exercises which reflects that 'competence stretching' is going on. The current mandate explicitly states that two exercises are hosted every year.[57] Another aspect is ENISA's progress in harmonization. Prior to ENISA, national and private initiatives took place in isolation of each other. This lead to diverging policies with different priorities and solutions. In order to establish an effective EU response these initiatives needed to be compatible with each other and meet certain requirements. This is why ENISA is the secretary of the Computer Emergency Response Team (CERT) community, who provide national protection, in order to establish trusted communication between countries and foster

[54] Council Conclusions 34/16, *European Council Conclusions* (15 December 2016).
[55] European Commission (2013)0027, *Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union* 28.
[56] Council Conclusions 187/21, *On Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry* (15 November 2016).
[57] ENISA, *Annual Activity Report 2017* 13-15.

cooperation.[58] Just like the EC3 it does not provide security per se but acts as a 'mechanism that enables stakeholders to work together'.[59]

ENISA and EC3 have a strong relationship built on mutual learning and collaboration to ensure a synergy and compatibility between the goals and objectives of each agency.[60] They act in semi-formalised arrangements to enhance cooperation and coordination capability to the benefit of the EU. In 2014 they signed a strategic cooperation agreement to cooperate more closely and exchange expertise formalized in the Joint Cybercrime Action Taskforce (J-CAT).[61] In 2005 and 2013 the Council opted to work more comprehensively on LEA cooperation. It recognized that the existence of gaps and differences in national legislation prevented optimal cooperation and asked EU institutions to 'approximate [harmonize] rules on criminal law in member-states in the area of attacks against information systems' and encouraged member-states to make use 'use of existing network of operational points of contacts' to prevent duplication of efforts.[62] Member-states were thus encouraged to use institutionalized platforms like ENISA and EC3 to enhance cooperation. The Council opted that cooperation could be 'better achieved at the level of the Union'.[63] These statements of the Council reflect the feedback loop mechanism. The statement of this body that cooperation should be achieved at EU level is immensely influential for institutions for their modus operandi. As this political body acknowledge the importance of cybersecurity institutions, little stands in the way of the Commission to propose policies to increase their competences to foster European cooperation.

EFMS – the European Forum for Member-States

Whilst ENISA and EC3 act as operational and consultative bodies, they do not encompass the political cooperation of cybersecurity. It is the 'European Forum for Member States' (EFMS) that does exactly this. The creation of the EFMS is exemplary for the 'critical juncture' of HI. This is because it was established in 2009 with the policy initiative on Critical Information Infrastructure Protection (CIIP) in response to the 2007 Estonia

[58] Dewar, *Cybersecurity in the European Union* 66.
[59] Schulze, M. & Bendiek A., 'The EU's revised Cybersecurity Strategy', *SWP Comments* (2017) Vol. 47(1) 4.
[60] Christou, *Cybersecurity* 12.
[61] ENISA, *Press release* 2014. https://www.enisa.europa.eu/news/enisa-news/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol
[62] Council Framework Decision 2005/222/JHA, *on attacks against information systems;* Council Decision 2013/40/EU.
[63] Council Framework Decision 2005/222/JHA.

cyberattacks. The 2007 cyberattacks was the 'branching point' for the EU as the current institutions ENISA and HTCC were not up to the task and thus the need to create a new institution. This was an incremental rather than a radical change as the EFMS was created in addition to the already existing institutions and it did not take away competences. The goal was to have an institution for high-level discussion between national representatives to foster political support and exchange good policy practices. The EFMS does not get involved in technical and operational issues – but asks ENISA and EC3 to provide this. Instead it complements and supports formal decision-making processes.[64] Its principal task is to identify critical infrastructure, evaluate the state of 'cybersecurity health' of the EU, to hammer out political agreement and to enable the EU to mitigate potential cascade or domino-effect of major incidents.[65] Its success derives from being a secure and effective cooperation mechanism to enable structured and coordination information exchange, detection and response at the highest political level. The EFMS received strong support at the Tallinn Ministerial CIIP conference of April 2009 and Council Resolution 2009/C 321/01 signalling the influence of positive feedback loop.[66] The EFMS is a remarkable flexible political organization and they meet on a quarterly basis. Their meetings are chaired by the Commission with ENISA as the secretariat. The member-states themselves may determine who to send as a representative as long as the maximum of three representatives is respected.

[64] Commission Staff Working Document (2013)32, *Impact Assessment* 97. http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_impact_ass_en.pdf p.97

[65] European Commission (2013)1, *Cybersecurity Strategy of the European Union* 16.

[66] Council Resolution 2009/C 31/01, *On a collaborative European approach to Network and Information Security.*

Chapter 4. The empirical analysis

This chapter surveys the progress of cooperation on cybersecurity matters in discourse and practice, with special attention to the progress of the more institutionalized expressions of this cooperation embodied by the EC3, ENISA and the EFMS. I describe the pre 2001 picture of the cybersecurity landscape first as prior to this date the EU installed its first cybersecurity initiatives. The earliest accounts of EU cybersecurity go back to the 1993 Commission Information Society policy paper known as the *Delors White Paper* and the 1994 Council Conclusions known as the *Bangemann Report*.

4.1 The EU cybersecurity landscape before 2001

The Delors White Papers urged the Community to focus on two development themes: the trans-European transport and energy networks and information networks.[67] It was understood that these emergent information technologies required Community guidance as the diversity of national approaches would mean an obstacle to the completion of the Internal Market and domestic legislation was ill equipped to allow for the highest level of security.[68] The Delors White Papers summed up a set of underlying principles for policymaking at Community level such as 'protecting privacy, intellectual property, commercial confidentiality and national security', which are regarded as the principles of the current cybersecurity strategy.[69] The entrepreneurial role of the Commission is influential enough to determine the principles of EU cybersecurity from 1993 onwards.

The Delors White Paper also urged member-states to ratify the Council of Europe Convention on Data Protection of 1982 – the first of its kind – as soon as possible since only seven member-states had done so.[70] However, the Commission did not have a single-purpose agency like ENISA to support cybersecurity coordination and policy development. A major concern at that time was also the absence of national

[67] European Commission, *Growth competitiveness and employment: the challenges and ways forward into the 21st century: white paper* (Brussel, 1993) 22.
[68] Ibidem, 22-28.
[69] Arnbak, Ax., *Any colour you like: the history (and future?) of EU Communications Security Policy* (Brussel, 2014) 4; European Commission (1990)314, Annex, Action line II, art. 2.1.7.
[70] The 1982 convention can be seen as the first attempt to institutionalize cybersecurity not within an EU context but within a wider geographical context. Coordination was to be promoted via article 13 which required each 'Party' (member-state of the Council of Europe) to assign national cybersecurity agents. These agents would exchange 'information on its data protection laws' under the supervision of the General Secretariat. Coordination during a cyberattack was not mentioned as there were no provisions to clarify the roles and responsibilities in such an event. Article 16 endorsed the General Secretariat with the power to overrule a Party if its agent refused to exchange information if that information was necessary to achieve data protection. This institution had a strong position vis-à-vis its member-states as it could overrule national decisions.

cybersecurity authorities who would cooperate together. Tackling cybercrime was carried out on a bilateral basis which proved to be difficult when it affected more than one member-state which necessitated the need for coordination of various Law Enforcement Agencies (LEA). For this purpose Europol was established in 1998. Earlier attempts to establish bodies to support the coordination of cybersecurity did not generate sufficient support. The Commission proposed to appoint a consultative group of senior officials called the 'Senior Officials Groups on Information Group' (SOG). The SOG would consist of member-states representatives and would advise the Commission on how to best achieve coordination and information-sharing.[71] This SOG could be considered a first attempt to institutionalize cybersecurity insofar as it would offer a place for policymakers to meet. Next to this consultative body, the Commission wanted to legally compel member-states to cooperate by obliging authorities from other member-states to perform tasks of another member-state if that member-state failed to provide sufficient data security. The SOG would be asked to facilitate this process.[72] This proposal and the SOG can be considered as a first attempt to institutionalize cybersecurity cooperation within the EU. The Commission took a hard stance on the coordination of cybersecurity which attracted criticism from the Council.

According to the Council, member-states would be obliged under Community Law to disclose possible sensitive national security information in order to collaborate and exchange cybersecurity information. This was seen as infringement from the Community on the member-states competences because it could not chose to disclose information voluntary.[73] The Council reacted with the *Bangemann Report*. This report would only allow a Community build-up of institutions and agencies who would focus on the primary competences of the Commission: the area of competition, protection of intellectual property and research & development. It should not concern itself with information security of the member-states. The Council countered the Commission's proposal with considerable alterations: the Council to have the final say in conflicts, more representation of member-states in expert groups and the right to suspend actions

[71] Unfortunately, I was unable to retrieve the actual mandate as it is missing in the EU archives. Therefor I can only make statements on the outline of the mandate that are based on the criticism of the Council. After a careful search and communication with the EU archive services, I received a message that the document I requested is lost and its file cannot be retrieved.
[72] European Commission (1990)314, 16.
[73] European Council, *Europe and the global information society – recommendations from the Bangemann Group* (Luxembourg, 1994) 33-35.

suggested by the Commission.[74] On terms of coordination and information-sharing the *Bangemann Report* is clear. It states that optimal information-sharing was seen as indispensable for a future-proof Community and this should be based 'on the appointment of a person at the ministerial level for coordinating all aspects of the subject'.[75] However, it was silent on who of the institutions (Commission, European Council, the Council) should spearhead this process and consequently the SOG was not used. Due to this situation no institution came up with credible alternatives for a Community-wide information system that would allow member-states and national authorities to share and coordinate information securely. Information-sharing and coordination would still be based on bilateral agreements with no institution to encourage this on a European scale.

4.2 The European approach and the small steps to institution building between 2001 and 2006

At the beginning of the millennia the Commission was concerned with the proliferation of criminal online activities.[76] The EU cybersecurity landscape leading up to the 2001 NIS proposal was characterized as a 'maze of non and legally binding instruments that raise legal and operational barriers that inhibit coordination'.[77] The missing link was the absence of a unified approach based on a pan-European thinking covering all NIS issues that would specify which instruments could facilitate coordination. This was exactly the aim of the 2001 *Network and Information Security: Proposal for a European Policy Approach*.

The NIS Proposal was a first attempt to codify this policy field and did so based on four pillars: a detailed typology of threats emanating from cyberspace, specific solutions to address these threats, provide a strict definition of Network and Information Security and it formalized actor cooperation at the centre of EU cybersecurity policy. At closer examination the text is remarkable prescriptive in nature as to specify particular solution to particular problems. For example it argued that interception of communications could only be avoided when operators adopt the

[74] Arnbak, Ax., *Any colour you like* 5; + Council Decision 92/242/EEC, *In the field of security information systems* (31 March 1992).
[75] *Bangemann Report,* 131.
[76] European Commission (2001)298, *Network and Information Security: Proposal for a European Policy Approach* 2.
[77] European Commission (2002)263, *eEurope 2005: an information society for* all; European Commission (2000)890, *Creating a safer information society by improving the security of information infrastructures and combating computer-related crime.*

measures from Directive 97/66 and extent DNS protocols when under attack or specified that anti-virus software should be used to combat this.[78] It is unusual for the EU to specify recommendations in such detail. Until this point the EU did not issue practical guidelines but instead raised awareness of potential risks so the actors involved could make their own choices. The proposal reflects a hands-on approach in which the EU was so confident in its ability that it issued a NIS definition for the first time in EU policy. According to Klimburg & Tiirmaa-Klaar the EU did this in order to address the fragmentation and lack of initiatives and cohesion in legislation the EU suffered at the time of the proposal.[79] The proposal is also remarkable about how the Commission perceived the concept of security. Because the Pillar Structure of Maastricht in 1992 laid down provisions in which the Commission could only address cybersecurity issues with an economic character and Justice and Home affairs provisions to address criminal activities were outside the its scope, the Commission argued that security itself was a commodity that could be bought and sold on the market.[80] This developed into a rationale that the Commission could focus only on cybersecurity with a financial/economic lens.[81] If we look ahead with the development of ENISA, we can argue that it started as an economic cybersecurity expert as the Commission competences allowed this and later stretched its competences to host exercises, guide NCSS development and operational responsibilities. This is remarkable as the Commission competences are primarily financial and economic and might suggest that the institutions and agencies are more flexible in stretching their competences than the Commission is.

The Commission illustrated that the EU cybersecurity landscape was fragmented and riddled with complexities. Some member-states were already developing their own form of cybersecurity policy (with Belgium being mentioned in the proposal) whilst others were not. This divergence caused concern as this would mean that the security of goods and services varied across borders therefore fragmenting the Internal Market. The Commission mentioned that engineers were surprised by the novelty of some incidents and attacks and noted that only a few member-states installed CERTs to address cyberattacks. However, even between these CERTs cooperation was difficult due

[78] European Commission (2001)298, 20.
[79] Klimburg, A. & Tiirmaa-Klaar, H., *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU* (European Parliament, 2011) 11.
[80] European Commission (2001)298 2.
[81] Dewar, *Cybersecurity in the European Union* 110.

to different operational parameters and levels of expertise.[82] In order to address this situation the Commission would use a top-down approach to increase cooperation. The Commission intended to examine 'how to best organize at European level data collection, analysis and planning of forward-looking responses to existing and emerging security threats'.[83]

Between 2001 and 2005 the HTCC and ENISA were created in order to provide this guidance and advice at the European level. They enable authorities to coordinate their information and provide guidelines and expertise; the HTCC on cybercrime and ENISA on legislation and policies. The objective was to become 'a centre of expertise at the European level' to provide advice, assistance and guidance.[84] The HTCC assisted the Commission to develop the EU Forum on Cybercrime in 2001 to enhance mutual understanding and cooperation at EU level between relevant actors. The HTCC held workshops and gave presentations about cybercrime.[85] The forum was a chance for the Commission to understand the needs from the private and public sector for legislation and it could thus spearhead policy development.

I looked up the first two years of ENISA's existence and this shows an interesting track record. Between 2004 and 2006 the agency was predominantly focused on relationship building with other institutions and the member-states by making visits to present and clarify its activities. This period was about getting to know the other players and being recognized as a value-added agency but it was also an uncertain period because it was not until 2006 that its legal basis was clarified and confirmed by the European Court of Justice.[86] Despite this uncertainty the agency was able to bridge the gap between governments and the private sector and encouraged a dialogue about responsibilities, roles and solutions which led to 140 requests for expertise and assistance from EU institutions and member-states about cybersecurity.[87] It is remarkable that so much was asked from an agency whilst its legal basis was not clarified. However, according to SI this is not unremarkable but highly predicted. As the cybersecurity community is relatively small, the process of socialization is quick when

[82] European Commission (2001)298 21
[83] Ibidem, 22.
[84] Council Regulation 460/2004, art II.
[85] European Commission (2001), *Commission organizes Forum on cybercrime* http://europa.eu/rapid/press-release_IP-01-1664_en.htm
[86] European Commission (2006), *ECJ confirms legality of the established ENISA* http://europa.eu/rapid/press-release_IP-06-567_en.htm
[87] ENISA, *General Report 2006* 10.

actors become acquainted. They share their expertise and policymakers realize the potential of ENISA as a coping mechanism and use it.

Its role vis-à-vis the member-states was especially significant when countries joined the EU. When Romania and Bulgaria joined the EU on 1 January 2007 these countries already had CERTs installed thanks to the help of ENISA who facilitated the transfer of Hungarian hands-on experience to these countries which had almost no cybersecurity policies.[88] The cybersecurity strategies of Romania and Bulgaria are also very positive to EU involvement which may highlight that the newer a state is to an unknown subject, the more positive it is to using services that it does not have domestically. In 2006 it was recognized that ENISA did contribute to cybersecurity questions and it set up a network of National Liaison Officers (NLOs) to enable efficient information exchange. This network was helpful in providing material for the 'country pages' that ENISA had setup. These pages serve as a platform for member-states to inform stakeholders about contact points and to offer updates, reports etc.[89] This was a first step in creating a 'hub' for exchanging cybersecurity information. The number of achievements illustrates that ENISA is a highly cost-effective organization considering its limited staff resources.[90]

4.3 The holistic approach and build-up to a recognizable cybersecurity policy between 2006 and 2013

Where the 2001 NIS Proposal focused on actor cooperation, the 2006 *Strategy for a Secure Information Society – 'Dialogue, partnership and empowerment'* (SSIS) centralized the concept of 'Holistic Approach'. A holistic approach meant that the EU would develop a cooperative environment in which relevant public and private actors would be invited to join and their respective roles recognized. This would in turn lead to a 'multi-stakeholder dialogue' based on partnership, empowerment and trust that would foster cybersecurity awareness, cooperation and a culture of cybersecurity.[91]

The SSIS was based on three pillars; specific NIS measures, a regulatory framework for communications and the fight against cybercrime. These pillars have their origins from the NIS Proposal but there is a sharp contrast between the 2001 and 2006

[88] ENISA*, General Report 2007* 22.
[89] ENISA, *General Report 2006* 10.
[90] ENISA, *General Report 2006* 11.
[91] European Commission (2006)251, *A Strategy for a Secure Information Society – Dialogue, partnership and empowerment* 6.

EU discourse. In 2001 the EU had a hands-on mentality and more or less dictated what action public and private and consumers should take to increase cybersecurity. Its discourse was about 'urgency', how member-state 'should' and 'must' ensure cybersecurity. Operators should secure networks 'as they are required to do under Directive 97/66 EC on Data Protection in Telecommunication'.[92] In 2006 the EU takes on a softer stance. It presents itself as a 'facilitator' of dialogue that 'invites' member-states to participate in 'partnerships of empowerment' in order to develop 'trust' and it presents ENISA as an agency that '*could* serve as a centre of information-sharing'. Instead of highlighting the formal relationship between the member-states and the institutions, the Commission speaks of 'stakeholders' on an equal footing who have 'mutual interests' and who will 'recognize their respective roles'. The background of this change was the political climate in which the SSIS was developed. Prior to 2006 there was a growing wariness of EU overextension that culminated into the 2005 Constitutional Crisis.[93] This forced the EU to switch its hard approach with regulations and directives towards a softer approach by encouraging member-states and about emphasising the normative impact of institutions.

It was ENISA who would be the carrier of the EU's softer message. It would facilitate the dialogue between stakeholders, foster cybersecurity culture, coordinate information-sharing and exchange best practices.[94] Operational coordination was to be put to the test via annual exercises coordinated by ENISA to benchmark national NIS-related policies to identify the most effective practices.[95] The EU-wide information system that was envisioned in 1990 and 2001 was given a green light an handed over to ENISA to spearhead the development of a 'European multilingual information sharing and alert system'. This system would integrate national public and private cybersecurity systems together via an 'e-security web portal'.[96] Information-sharing was thus being institutionalized and its management given to the EU agency. The SSIS linked a connection between a European problem and a solution. The problem was an absence of a culture of security that inhibited a well-coordinated European alert system in the event of cyberattacks, no clear understanding of best practices in cybersecurity policies and a lack of trust between stakeholders. To address this at a European level was

[92] European Commission (2001)298 10.
[93] Pawlak, P., 'Politics of cybersecurity capacity building: conundrum and opportunity', *Journal of Cyber Policy* (2016), Vol. 2(1) 130.
[94] European Commission (2006)251, 11.
[95] Ibidem, 13.
[96] Ibidem, 14.

considered as the best option as ENISA could facilitate the dialogue and coordination to ensure European capability against cyber threats.

The EU cybersecurity landscape experienced an earthquake with the 2007 Estonia cyberattacks. In 2007 a series of cyberattacks targeted Estonian websites of banks, parliament and ministries. The main type of attack was the denial of service (DoS) which means that a website is overloaded as the servers cannot process all the data and the website is (temporary) shut down. Although the material impact of the attack was minor, the political fallout was significant as the attack illustrated that a highly-developed state could be shut down with such a sophistication that it implied state involvement.[97] Estonia was inclined to invoke article V of the NATO Treaty and if the article was triggered the consequences would have been severe. The attack thrusted cybersecurity into the political domain and spurred activity at the highest level of EU decision-making especially in the area of CIIP. It was recognized by the EU that cyber aggression was a potent issue and concentrated its efforts to secure cyber infrastructure. The EU placed particular emphasis on the information exchange between the national cybersecurity authorities and called for the improvement of cooperation mechanisms. A content analysis of relevant EU acquis published between 2007 and 2013 shows how CIIP became crucial in EU cybersecurity policy and demonstrates the willingness of the EU to act. In this period of the 73 documents that were published over 20 addressed CIIP including two Commission Conclusions and three Council Conclusions.[98] The attack spurred the development of the European Forum for Member-States (EFMS) in order to ensure high-level cooperation and information and intelligence sharing between national authorities in the event of cyberattacks.

The role and impact of the cybersecurity institutions were influenced by the events of 2007 and between 2007 and 2013 we see an acceleration in EU discourse to use institutions. This discourse is about adjusting their modus operandi and responsibilities in order to allocate competences to these institutions to strengthen the cybersecurity landscape. This started with the Commission Communication on *Critical Information Infrastructure Protection* in 2009. Where the SSIS narrative was more member-state friendly, the 2009 Communication's narrative was about the dangers of cyberspace being used by warmongers and terrorists and that security of CIIP reflected

[97] Clingendael Institute, *Foreign Policy Responses to International Cyber-attacks – some lessons learned* (The Hague, 2015) 4.
[98] Dewar, *Cybersecurity in the European Union* 60.

the 'frontline' of EU cyberdefence.[99] More EU coordination and cooperation was 'the way forward' in order to build a robust and resilient EU cybersecurity landscape. The Communication suggested that events like Estonia could have been mitigated when preventive measures were coordinated via structured information-sharing instruments and venues to exchange good practices. ENISA and the EFMS were positioned as being the actors that could offer the right assistance but only if member-states accepted the added-value of these agencies by ENISA to develop pan-European coordination schemes (e.g. CERT), the European warning system and member-states to systematically participate in cybersecurity exercises. The Communication can be considered successful as *Council Resolution 2009/C 321/ on a collaborative European approach to Network and Information Security* acknowledged the importance of ENISA to foster a culture and act as the centre of expertise.[100] The resolution provides room for the Commission to carry out performance management in the field of cooperation. The Commission is invited to come forward with new proposals about a reinforced and flexible mandate for ENISA to reach a 'strengthened oversight over the Member States'.[101] This is a remarkable sentence as it suggests that previous oversight by ENISA was inefficient and that the Council wants to keep its own members in check. This sentence suggests two things: member-states come to an understanding that they should give more competence to ENISA to reach the common goal of EU cybersecurity and the commission is successful in positioning its agency as the right actor for this and this is taken over by the Council. What this resolution shows is the partly confirmation of the HI theory, with its feedback mechanism, and the SI theory with its coping mechanism. Like the passage about 'strengthened oversight', the text is full of references to the strengths of ENISA, namely to provide expertise and knowledge. This is visible when we note chapter VI of the resolution. The Council wants member-states to organize or participate in exercises, create CERTs, increase efforts in education and training and to react jointly in a cross-border incident. This is difficult to accomplish due to the 'complexity of the area', 'involvement of various stakeholders' and 'sensitivity of the topic'. ENISA is then positioned by the Council itself as the right actor to assist and states that it is ENISA that 'should serve as the EU's centre of expertise in EU related NIS matters'.[102] This statement is the positive feedback loop in which the agency is perceived as the right

[99] European Commission (2009)149, *On Critical Information Infrastructure Protection (CIIP)* 10.
[100] Council Resolution (2009/C 321/01) 4.
[101] Ibidem, 4.
[102] Ibidem, 3.

actor and the Council sees ENISA as a coping mechanism to cope with the complexity of cybersecurity. At further inspection the resolution also reflects the RCI theory. The Council mentioned that member-states should use the institutions and refrain from setting up new bodies. This is linked with the 'transaction costs' mechanism because to make use of existing platforms reduces cost and to pool resources together.

All three of the cybersecurity institutions worked extensively together as we can see from the annual reports in which they all highlight the extent of their interagency cooperation. EFMS and ENISA developed a common methodology on critical information infrastructure which is important as to ensure the same level of security for infrastructures throughout the EU, ENISA developed three more CERTs units and Europol noted a staggering increase in cybercrime collaboration with EC3.[103] Efforts in hosting annual exercises were paying off as ENISA noted that the 2011 'Cyber Atlantic' exercise was marked by excellent cooperation within the EU and between the EU and the US.[104]

4.4 Competence stretching and the permanent institution of ENISA between 2013 and 2018

Between 2013 and 2018 two documents were published that represent the 'critical juncture' mechanism of the EU cybersecurity landscape. The first is the 2013 *European Union Cybersecurity Strategy (EUCS)* and the second is the 2018 *Cybersecurity Package*. They influenced the manner in which the cybersecurity institutions would run a future EU cybersecurity landscape.

The EUCS led to the strengthening of cybersecurity management at the EU level. This second cybersecurity strategy, SSIS being the first, reaffirmed the role of the EU as a facilitator of operational and strategic coordination. The EU would help to raise awareness, achieve cyber resilience, support national policies/strategies and would be involved in the case of cyber-attacks or incidents. It specified the roles and responsibilities of member-states and EU actors involved which indicates that the EU had now more confidence in its abilities than during the SSIS in 2006 to develop a long term strategy and gets serious about cybersecurity. This seriousness also translates into the first ever mentioning of the EU to develop its own cyber-defence capabilities which reflect the political mood at the time that a series of cyber incidents suggested state

[103] ENISA, *General Report 2013* 17; Europol, *General Review 2012* 39.
[104] ENISA, *General Report 2007* 15.

involvement. It might also show that this time the EU was faced with an external crisis rather than an internal one that created a vacuum for the EU to step up its game.

On a policy level the EU would protect cyberspace by the application of its core principles within cyberspace. First, freedom and openness would be achieved by applying the EU's core values and rights in cyberspace. Second, laws and norms would be applicable in cyberspace. Third, cybersecurity capacity building would allow the EU to engage with international organizations and partners. Fourth, the strategy was aimed to foster cooperation and trust in cyberspace. The issue of trust is noteworthy as institutions invest much effort in developing confidence building measures to increase or maintain trust. Three national strategies (France, Romania and the Netherlands) indicate that the issue of trust between actors and with cybersecurity is the most persistent issue. For that reason all member-states develop measures to enhance trust.[105] In the reports of ENISA and EC3 the issue of trust between actors appears to be a top priority. According to Europol to build trust is to 'enhance the capacity and capabilities of LEA's'.[106] And ENISA's reports on confidence-building measures in the non-nuclear energy infrastructure was taken over by the Organization for Security and Cooperation in Europe (OSCE).[107]

The EUCS was influential because it was more coherent than previous policies which were more standalone products. It drew elements from other EU policy strategies (Internal Security Strategy 2010, Stockholm Programme 2010 and Digital Agenda 2013) together that enabled the EU to develop coherence and move forward with a single strategic vision.[108] The EUCS plus the NIS Directive provided a cooperative framework that would encourage member-states to work together more frequently. Like previous cybersecurity policies, the EUCS emphasized EU coordination to solve the fragmentation of national policies. The EUCS positioned ENISA as the right actor in the right place to oversee the management of cybersecurity which only needed a modernized mandate with extra competences. This mandate was approved on April 16 2013.[109]

---

[105] For the French it is the 'Expert Panel for Digital Trust', the Dutch the 'Digital Trust Center' and for Romanians the 'Mutual Trust Center' which all make references to ENISA as an important stakeholder.
[106] Europol, *Annual Review 2017* 34.
[107] ENISA, *ENISA Cyber security studies widely cited by OSCE* https://www.enisa.europa.eu/news/enisa-news/enisa-cyber-security-studies-widely-cited-by-osce
[108] Dewar, R., 'Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union Cybersecurity Policy' (Conference Proceedings, 2015) 14.
[109] ENISA, *Green light for new regulation for EU cybersecurity Agency ENISA given by the European Parliament* https://www.enisa.europa.eu/news/enisa-news/green-light-for-new-regulation-for-eu-cyber-security-agency-enisa-given-by-the-european-parliament

The importance of cybersecurity between 2013 and 2019 persisted and in 2017 the President of the European Commission Jean-Claude Juncker called cybersecurity the top priority for the EU's future in his annual State of the European Union Address.[110] The EU's ambitions and plans towards cybersecurity culminated in a surprisingly detailed communication entitled *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. Once again EU's discourse on cybersecurity included strong vocabulary not seen prior to 2013 with words like 'resilient', 'deterrence' and 'defence', terminology most commonly associated with national (defence) strategies. The Communication proposed a new law known as the *EU Cybersecurity Act* which included a new EU cybersecurity certification framework and a permanent mandate for ENISA. If approved the law would mean that all its regulations would be directly applicable in all member-states and new competences to ENISA. On December 10 2018 the European Parliament, the Council and the European Commission reach a political agreement on the *Cybersecurity Act* propelling its cybersecurity management forward.[111] When the Act was approved it automatically accepted the *Cybersecurity Package* that comprised of a number of *Communique* of which the *Cybersecurity Act* and the *EU Cybersecurity Blueprint* are the newest policy documents of the EU.

With the acceptance of the *Cybersecurity Package*, ENISA transformed into the cybersecurity agency the EU envisioned since its creation. The fact that the EU now calls ENISA its 'cybersecurity agency' is the parameter for the affirmation of the agency's skills and purpose. 'Competence stretching' and 'positive feedback' are visible within the *Blueprint* and the *Act*. ENISA again gets the recognition from the Council, the Commission and the industry as being the 'centre of expertise': its ability to overcome policy gaps between member-states and to build synergy between the industry's need for supportive cyberlegislation and the member-state's realization of the 'skill gap' between cybersecurity knowledge within the public domain and the private.[112] The latest survey conducted by ENISA in 2017 affirms this recognition and puts forward some examples of its achievements: an EU cybersecurity research and competence centre, co-developed a cyber-emergency fund, given trainings and workshops and 24 member-states use guidelines from ENISA to promote confidence-building measures.[113]

---

[110] European Commission, *State of the Union Address 2017.*
[111] European Commission (11 December 2018), *Agreed! EU Cybersecurity Act* https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en
[112] European Parliament (2019)0151, *EU Cybersecurity Act* art. IV-VI.
[113] ENISA, *Annual Activity Report 2017,* 20.

In terms of competence stretching, three important shifts will occur in the day-to-day performance management of member-states with the implementation of the *Act* and the *Blueprint*. The first is the incident reporting by member-states, the second is the certification scheme and the third is the operational management in case of cyberattacks on grand scale. Prior to the *Act,* a number of reporting schemes existed and this fragmented the existence of one solid overview of all cyberattacks and incidents. Thus ENISA developed the *Technical Guidelines* to report cyberattacks and incidents based on a single methodology. However, this was still voluntary for member-states to use which did not prevent further fragmentation. The *Act* made it mandatory for member-states to use the *Technical Guidelines* for incident reporting. This extra competence of ENISA to provide this knowledge is important for the EU institutionalised landscape. Because cybersecurity is about data, the data-purity of incidents and attacks is important to manage cyberattacks and incidents and make judgements. This in turn allows the EU to have a better understanding of the weaknesses in its infrastructure. Secondly, the ICT certification schemes. These schemes show the level of cybersecurity of ICT products and services. Prior to the *Act*, a multitude of schemes existed and there was no harmonization between the national schemes and this led to the situation where a high security label was not automatically recognised as the same level in a different member-state. This was considered a distortion of the market and could invoke Union action. The *Act* gives ENISA the sole competence to develop EU wide certification schemes and it tries to prevent member-states from introducing new schemes as this would distort the Digital Market. Union law lays down minimum requirements for ICT products and services and member-states are obliged to enforce the legislation.[114] This in turn gives the EU more control over the socio-economic aspects of the Digital Market to ensure Union-wide cybersecurity via ENISA.

The third shift is the operational management during cybersecurity incidents and is the biggest competence stretching of ENISA. In the event of a large-scale cybersecurity incident involving more than two member-states, the *Blueprint* is triggered, and ENISA has operational responsibility to coordinate a response.[115] ENISA is informed within 24hrs of the incident and can activate nine phases to inform national and EU actors. Each phase adds more operational competences to ENISA to call upon necessary national and institutional bodies (e.g. EC3 and EFMS) to provide support or execute tasks as the

[114] European Parliament (2019)0151, *EU Cybersecurity Act* art. IV-VI.
[115] European Commission (2017)6100, *On Coordinated Response to Large Scale Cybersecurity Incidents and Crises* 15-19.

situation progresses. This chain shows which actors are supposed to do what at different levels (local, national, regional and supranational). At the supranational level we see the strategic and political actors active. When the situation requires a strategic and political answer (e.g. 2007 Estonia cyberattacks), ENISA informs the Council and Commission who judge if to enact the 'Cyber Diplomatic Toolbox' which allow member-states to invoke the *Mutual Defence Clause* to provide a wide array of (military) assistance.[116] If a single region is affected ENISA calls its partners in regions untouched to bolster their security via its 'European Warning and Information System' or to reroute resources to the affected region. At the national level EC3 informs LEA's with, if possible, the location from whereby the attack/incident is coming from. They can then execute the shut-down operation at the local level. When the pre-attack/incident situation is achieved, ENISA will do an inquiry for best practices cases and the EFMS will evaluate the affected infrastructure. This new competence is the biggest achievement of EU cybersecurity coordination since the creation of ENISA. As operational command is normally associated with national elements, this suggests two things: the affirmation of the member-states that in order to cope with cybersecurity attacks/incidents, European oversight is needed to coordinate EU wide resources to handle the situation. It also affirms the notion that the boundaries between national and European lines do not matter with cybersecurity and they become blurry in which a strict national or European viewpoint is ill-suited to cope with cybersecurity issues.

The *Blueprint* is a detailed document delineating the roles and responsibilities of those involved but it also reflects a rather naïve mentality. Scenario's in strategies or drills are promising in times of tranquillity when a particular framework is set. The crucial element here is that drills and strategies are staged which means that they are invented and thus follow a predetermined path. However, incidents and attacks do not follow a certain path or abide by the scenario timetable and they certainly do not wait to move until the EU has activated the next phase. In that sense the *Blueprint* represents a simple attitude towards something so complex as cybersecurity incident management. Every plan, strategy and scenario acknowledges its flaws and expects the presence of 'unknown unknowns' and it is not its sole purpose to manage the attack/incident in order to return to the pre-attack situation. Strategies and exercises are about guidance and the allocation of responsibilities, indicating that there is more than one actor involved. This group effort needs cooperation in order to have a chance of success. That

[116] Ibidem, 3.

is why the core objectives of the *Blueprint* starts with the aspect of cooperation; it is about who, at the local up to the supranational dimension, does what in a certain situation without an explicit assurance that the strategy will succeed.

Conclusion: connecting the dots

This thesis opened with a comment on *The Cornfield* painting of John Constable and made a connection between this painting and the institutional landscape of the EU. Whereas men and animals thrive when they take care of nature, so we must see the correlation between institutions and member-states as well. Institutionalisation progresses when member-states and institutions take good care of each other and cooperate on good terms. In terms of cybersecurity, this was the aim of the EU since the publication of 1993 *White Paper*.

It was the central aim of this thesis to understand how EU cybersecurity institutionalisation developed between 2001 and 2018. In doing so, it used the theory of institutionalisation and the mechanisms 'competence stretching', 'feedback loop' and 'Entrepreneurship of the Commission' to look for evidence of this process and put the agencies EC3, ENISA and the EFMS under review. Institutionalism takes the institution as the unit of analysis and claims that institutions matter. They matter as they offer benefits to member-states and gain competences as institutions bring benefits to member-states. This study aligned with the statement on institutionalism and shows how institutions developed over time to take on extra competences and become more influential and important to member-states.

The timeframe (2001-2018) of this study represents three different periods with each a different EU mentality. At first we see rapid institution-building between 2001 and 2016 with the creation of HTCC (2002) as the predecessor of EC3 and ENISA (2004). The NIS Proposal of this period reflects the mentality of the EU back then. The EU narrative was top-down with detailed information about how to achieve cybersecurity and the way forward was to build institutions. Institutions like the HTCC and ENISA spent a lot of time consolidating their position and gaining recognition for their work. This was met with some resistance from the member-states who wanted to keep control of the institutional trajectory. This is why during 2006 and 2013 there were pushbacks to EU policies and consequently it had to change its narrative to the 'concept of holistic' approach with the SISS in which the supportive roles and coordination efforts of institutions were emphasised. The creation of the EFMS in 2009 may also be connected to the desire of member-states to regain control of institutionalisation, next to the logical benefits of cooperation on cyber infrastructure. As to control cybersecurity infrastructure is nationally vital, to hand out this power to an institution may be undesirable from a rational member-state point of view.

In adjacent to this development, this period also experienced consolidation of institutions as member-states slowly but surely acknowledge the importance of cybersecurity institutions to promote coordination, create a culture and be a point of reference. It was the third and final period between 2013 and 2018 that witnessed the extension of competences and authority of institutions over member-states. In the beginning member-states had control over their own cybersecurity strategy. With the acceptance of the EUCS, member-states have to coordinate their policies with ENISA in order to align with EU objectives. If there were no CERTs units in place, ENISA brings in expertise to build this network. The most recent piece of evidence suggesting institutionalism expanding rapidly is the *Cybersecurity Act* that brought about a shift in EU focus of cybersecurity from purely economic issues to more security-based cooperation when ENISA gained operational command in the event of transnational cybersecurity attacks. The member-states approved and encouraged this development as the expertise and influence of institutions become more paramount. Member-states refrain from creating more institutions as they knew it would further fragment an already complex policy area with numerous stakeholders.

The given timeline represents the notion of change. Change is at the heart of institutionalisation as member-states and institutions constantly change to adapt to each other's new position and competences. This study finds that change occurs because of internal or external triggers. The Constitutional Crisis of 2005 can be seen as an internal trigger as this resulted in a shift in EU mentality from a top-down to a supportive narrative. The EU stressed the importance of its institutions as 'facilitators' of cybersecurity dialogue, as knowledge centres and to exchange best practices. This is the period of the 'holistic approach'. The 2007 cyberattacks are a clear example of an external trigger. The material impact was low but the political impact was high. The result was a change in discourse. The EU moved from an appeasing attitude to a more affirmative, reactionary and hardened stance. This shift was accompanied with the creation of a new cybersecurity institution (EFMS), an EU strategy with a military like narrative that obligated member-states to develop strategies and the realisation of member-states of the collaborative impact institutions can have on the overall security of the EU. This realisation was officially recognized by the Council Resolution of 2009 distinctively named 'a collaborative European approach' and recognized ENISA as a centre of expertise to foster a cybersecurity culture.

The analytical framework

The three mechanisms that were used during this research show how institutionalisation can be visualised. The competences have improved progressively well between 2001 and 2018. For example, ENISA has grown from a small agency with a limited budget and a strict mandate focused only on socio-economic issues, to a real mature cybersecurity agency with more staff and big budget. Its mandate is now permanent and incorporates operational aspects in the event of transnational cyberattacks and strategic elements with the creation of cybersecurity strategies and CERTs units. It is not unlikely that it will take on cyberdefence issues as it signed a 'Memorandum of Understanding' with the European Defence Agency, EC3 and the CERTs to establish a cooperation framework.[117] This memorandum shows the willingness of ENISA to be informed and talk about civic-military cooperation in the field of cybersecurity and defence. For now this is too far-fetched, but cybersecurity easily transcends the boundaries between civic and military making it an understandable choice to not just be an expert on civic cybersecurity, as ENISA currently is, but also become an expert on military cyberdefence and pool expertise together. The institutions are seen as epistemic communities in which the process of socialization gives credence to the build-up of a coherent cybersecurity culture. Precisely because of this expertise member-states listen to institutions because they trust their knowledge based judgements.

The second mechanisms that is visible is the feedback loop. Positive feedback from the member-states about the functioning of the cybersecurity institutions have made it possible for the Commission to foster tighter cooperation within proposals and strategies. Because member-states in general regarded the institutions as something positive and external triggers showed the urgency of cooperation, the Commission was able to pass forward proposals like the EUCS and the Cybersecurity Act with more ease. This situation combined with the activity of the Commission to build stronger institutions during this period, as it constantly tried to develop its policies with reports, recommendations and legislative acts to push for changes in mandates to have stronger institutions, allowed for a vacuum in which institutions gained immensely. The Commission was able to frame external crisis like the 2007 cyberattacks as a fundamental flaw of all member-states and that much could have been prevented if more cooperation via the EU framework would have happened. It is the Commission that

[117] ENISA, 'Four EU cybersecurity organisations enhance cooperation' May 23 2018. https://www.enisa.europa.eu/news/enisa-news/four-eu-cybersecurity-organisations-enhance-cooperation

shapes the narrative of the EU in a more softer tone with the SISS of 2006 and the more reactionary and active language with the EUCS in 2013. We have witnessed a tremendous growth from non-existing institutions in the pre-2001 era up to the *Cybersecurity Act*, which is in effect since 27 June 2019, with three cybersecurity institutions firmly embedded within the EU cybersecurity landscape and are here to stay and will likely strengthen their competences.

The theory

The evidence above gives credence to historical institutionalism and sociological institutionalism. Central to HI is continuity and path dependency and central to SI is norms building and the issue of coping. Within the period we see these two aspects develop. From the earliest accounts of cybersecurity with the *Bangemann Report* or the *NIS Proposal* in 2001 up to the *Cybersecurity Act* of 2019, we see continues change that actually highlights continuity. We also see a realisation of member-states that to work with institutions is the norm and legitimate as they offer knowledge and expertise to cope with the complexity of cybersecurity, institutions have developed a culture in which the epistemic community can transcend the national boundaries that may cumbersome cooperation. The continuity is the process of build-up and competence stretching of institutions. Prior to 2001 there were no cybersecurity institutions, and after a period of 18 years there exist three firmly embedded institutions in 2019. The apparent changes we see in policies, recommendations, external and internal triggers did not hinder competence stretching to a large extent. In fact, it is the other way around: thanks to external and internal triggers, the belief in institutions as a solution to cybersecurity non-cooperation gradually became stronger.

The evidence also shows that the power of the institutions to influence the preferences of states is great. The Commission, together with its cybersecurity institutions, has shown that the only logical way to deal with the cybersecurity is to cooperate in a framework that transcends national boundaries. The norms and values to deal with cybersecurity has changed within the thinking of member-states from a bilateral narrative towards a multilateral thinking in which working through an agency is considered the only legitimate and logic thing to do. It is not a coincidence that the EU has agencies for judicial cooperation (EC3), legislative/policy cooperation (ENISA) and political and strategic cooperation (EFMS). The EU supports institution building because it tightens the bonds between the EU and the member-states as the EU provides the know-how and expertise and it is up to the member-states to execute the tasks. To

this regard the 'entrepreneurial role' of the Commission must not be underestimated. It has published the colossal EUCS, pushed for the Cybersecurity Act and in all its documents showed the importance of institutions and pushed ENISA to the forefront of the European cybersecurity landscape. Without this support, ENISA would end up like the SOG: forgotten and not used.

We can safely suggest that ENISA is the profound winner in the institutional development between 2001 and 2018. Within a period of 14 years it developed from an agency based upon the idea to become a 'centre of expertise' and provide valuable information to member-states on economic cybersecurity issues, to the European Union's cybersecurity agency with a permanent mandate who has operational responsibilities in the event of transnational cybersecurity incidents, hosts international exercises, trains the CERT community, has strategic influence on member-state' cybersecurity affairs, and determines which products and services are secure enough to be sold on the internal market. Its original mandate did not have any of these competences although the last competences was probably envisioned as it was started as a purely economic cybersecurity institution. The case-study of ENISA suggests that the EU cybersecurity institutionalised landscape is at a particular crossroad where it jumps from a purely economic narrative towards a political, strategical and operational narrative on cybersecurity affairs. The fact that there is a proposal on the table to reform the mandate of the EFMS which include changing the name to 'Cooperation Group' shows just how much the element of cooperation is slowly and surely becoming the single factor within the EU cyber institutional set-up.[118]

Further research

This study has focused on three agencies within a twenty year timespan and tried to explain the development within a limited wordcount. It has succeeded in this to a large extent. However, it could present much more interesting results about the relationship between institutions and member-states if there was room to research policy convergence between the member-states. This would show if member-states are truly working together to achieve a common goal. This was not the scope of this thesis and thus further research is encouraged to look into this. One may start by conducting a comparative analysis between national policies to illustrate whether or not policy goals

118

between member-states are becoming similar. This does not only highlight the level of convergence but also divergence which is much more interested to understand.

Bibliography

Arnbak, Ax., *Any colour you like: the history (and future?) of EU Communications Security Policy* (Brussel, 2014).

Borzel, T. & Risse, T., 'Conceptualising the Domestic Impact of Europe' in: Featherstone, K., (ed.), *The Politics of Europeanisation* (Oxford University Press, 2003) 27-56.

Caporaso, P., *Theorizing Europeanisation* (Cambridge, 2008).

Cross, M., *Security Integration in Europe: How Knowledge-based Networks Are Transforming the European Union* (University of Michigan Press, 2011).

Chaudhary, T. & Jordan, J., 'Patchwork of confusion: the cybersecurity coordination problem', *Journal of Cybersecurity* (2018), Vol. 0 (0), 1-13.

Christou, G., *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Palgrave, 2016).

Clingendael Institute, Foreign Policy Responses to International Cyber-attacks – some lessons learned (The Hague, 2015).

Dewar, R., 'Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union Cybersecurity Policy' (Conference Proceedings, 2015).

Dewar, R., *Cybersecurity in the European Union: an historical institutionalist analysis of a 21st century security concern* (PhD dissertation, 2017).

Downing, M., The Military Revolution and Political Change: Origins of Democracy and Autocracy in Early Modern Europe (Princeton, 1992).

DiMaggio, P. & Powell, W., *The New Institutionalism in Organizational Analysis* (The University of Chicago Press, 1991).

Feiock, R., 'The Institutional Collective Action Framework', *Policy Studies Journal* (2013) Vol. 41(3), 397-425.

Goetz, K. & Hix, S., 'Introduction: European integration and national political systems' in: Goetz, K. & Hix, S., (eds) *Europeanisation Politics? European Integration and National Political Systems* (London, 2001) 1–26.

Hall, P., 'Political Science and the Three New Institutionalisms', *Political Studies* (1996), Vol. 44 (5), 936-957.

Hall, P., 'Politics as a process structured in space and time' in: Fioretos O (ed.), *The Oxford Handbook of Historical Institutionalism* (Oxford University Press, 2016) 31-50.

Hall, 'Political Science and the Three New Institutionalisms' 12; Shepsle, K., & Weingast, B., 'The institutional foundations of Committee Power', *American Political Science Review* (1987), Vol 81(1) 85-104.

Hall, P., 'Historical Institutionalism in Rationalist and Sociological Perspective' in: Mahoney, J. (ed.), *Explaining Institutional Change – Ambiguity, Agency and Power* (Cambridge, 2010) 204-223.

Krasner, S., 'Sovereignty: An Institutional Perspective,' *Comparative Political Studies* (1988) Vol 21(1) 66–94.

Klimburg, A. & Tiirmaa-Klaar, H., *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU* (European Parliament, 2011).

Ladrech, R., 'Europeanization of Domestic Politics and Institutions: The Case of France', *Journal of Common Market Studies* (1994), Vol. 32(1),69-88.

Lavenex, S., 'A governance perspective on the European Neighbourhood policy: Integration beyond conditionality?', *Journal of European Public Policy* (2008), Vol. 15(6) 938-955.

Lecours, A., 'New Institutionalism: Issues and Questions' in: Lecours, A. (ed) *New Institutionalism: Theory and Analysis* (University of Toronto Press, 2005) 3-26.

Levi, M., 'A Model, a Method, and a Map: Rational Choice in Comparative and Historical Analysis' in: Lichbach, M. (ed.), *Comparative Politics: Rationality, Culture and Structure* (Cambridge, 1997).

Lewis, J., 'The Janus Face of Brussels: Socialisation and every day decision making in the European Union, *International Organisation* (2005) Vol. 59(4) 937-971.

Lowndes, V., 'The Institutional Approach' in: Marsh, D. (ed.), *Theory and Methods in Political Science* (Palgrave, 2002) 66-79.

Marxsen, C., *Territorial Integrity in International Law* (Berlin, 2015).

Morrow, R., 'Education and the Postmodern Challenge', *Educational Theory* (1994), Vol. 44 (1), 43-61.

North, D., Institutions, Institutional Change and Economic Performance (Cambridge University Press, 1990).

Olsen, J. & March, J., Rediscovering Institutions: the organizational basis of Politics (Free Press, 1989).

Olsen, J. 'The Many Faces of Europeanization', *Journal of Common Market Studies* (2002), Vol.40(5) 923.

Pawlak, P., 'Politics of cybersecurity capacity building: conundrum and opportunity', *Journal of Cyber Policy* (2016), Vol. 2(1) 123-144.

Pierson, P., 'Increasing Returns, Path Dependence and the Study of Politics', *The American Political Review* (2000) Vol. 94 (2) 251-267.

Princen, S., 'Agenda-setting in the European Union: a theoretical exploration and agenda for research', *Journal of European Public Policy* (2007), Vol. 14(1) 21-38.

Rasmussen, G., 'Frames, agency and institutional change: the case of benchmarking in Danish construction', *Construction Management and Economics* (2017), Vol. 35(6) 305-323.

Robert, L., 'Europeanization and Political Parties: Towards a Framework for Analysis', *Journal of Common Market Studies* (2004), Vol. 52 (4), 573-596.

Schimdt. V., 'Democratic Legitimacy in a Regional State?', *Journal of Common Market Studies* (2004), Vol. 42 (4) 331-355.

Scheinder, G. & Ershova, A., 'Rational Choice Institutionalism and European Integration', *Oxford Research Encyclopedia of Politics* (Oxford University Press, 2018).

Schulze, M. & Bendiek A., 'The EU's revised Cybersecurity Strategy', *SWP Comments* (2017) Vol. 47(1) 1-7.

Smith, E., *Europe's Foreign and Security Policy: The Institutionalization of Cooperation* (Cambridge, 2004).

Thelen, K., 'Historical Institutionalism and Comparative Politics', *Annual Review of Political Science* (1999) Vol. 2 (3) 369-404.

Violakis, P., Europeanisation and the Transformation of EU Security Policy Post-Cold War Developments in the Common Security and Defence Policy (Routledge, 2018).

Weingast, B. & Marshall, W., 'The Industrial Organization of Congress', *Journal of Political Economy* (1988), Vol. 96(1) 132-163.

Weingast, B., 'Rational-Choice Institutionalism' in: Katznelson, I., *Political Science: The State of the Discipline* (New York, 2002) 660-692.

European Union sources

Commission Staff Working Document (2013)32, *Impact Assessment*. http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_impact_ass_en.pdf

Council Decision 92/242/EEC, *In the field of security information systems* (31 March 1992).

Council Regulation 460/2004, *Establishing the European Network and Information Security Agency*.

Council Framework Decision 2005/222/JHA, *on attacks against information systems*.

Council Resolution 2009/c 31/01, *On a collaborative European approach to Network and Information Security*.

Council Conclusions 34/16, *European Council Conclusions* (15 December 2016).

Council Conclusions 187/21, *On Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry* (15 November 2016).

Council Conclusions 14435/17, *Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (20 November 2017).

Directive 2011/92/EU, On combating the sexual abuse and sexual exploitation of children and child pornography.

Directive 2013/40/EU, *On attacks against information systems and replacing Council Framework Decision 2005/222/JHA.*

European Commission, *Growth competitiveness and employment: the challenges and ways forward into the 21st century: white paper* (Brussel, 1993).

European Council, *Europe and the global information society – recommendations from the Bangemann Group* (Luxembourg, 1994) 33-35.

European Commission (1990)314, Annex, Action line II, art. 2.1.7. http://aei.pitt.edu/3768/1/3768.pdf

European Commission (2001)298, *Network and Information Security: Proposal for a European Policy Approach*.

European Commission (2001), *Commission organizes Forum on cybercrime* http://europa.eu/rapid/press-release_IP-01-1664_en.htm.

European Commission (2002)263, *eEurope 2005: an information society for all*.

European Commission (2000)890, *Creating a safer information society by improving the security of information infrastructures and combating computer-related crime*.

European Commission (2004)401, *Communication from the Commission to the European Parliament and the Council: Area of Freedom, Security and Justice: Assessment of the Tampere programme and future orientations.*

European Commission (2006)251, *A Strategy for a Secure Information Society – Dialogue, partnership and empowerment*.

European Commission(2006)*, ECJ confirms legality of the established ENISA* http://europa.eu/rapid/press-release_IP-06-567_en.htm.

European Commission (2009)149, *On Critical Information Infrastructure Protection* (CIIP).

European Commission (2013)0027, *Proposal for a Directive of the European Parliament and of the Council. Concerning measures to ensure a high level of network and information security across the Union*.

European Commission (2013)1, *Cybersecurity Strategy of the European Union*.

European Commission (2017)6100, *On Coordinated Response to Large Scale Cybersecurity Incidents and Crises.*

European Commission (2017)476, *Communication from the Commission to the European Parliament and The Council: Making the most of NIS – towards the*

effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

European Commission (2017)450, *Joint Communication to the European Parliament and The Council: Resilience, Deterrence and Defence - Building strong cybersecurity for the EU*.

European Commission (11 December 2018), *Agreed! EU Cybersecurity Act* https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en.

European Commission, *State of the Union Address 2017*.

Europol, *Annual Review 2010*.

Europol, *Annual Review 2012.*

Europol, *Annual Report 2013*.

Europol, *Annual Review 2017*.

ENISA, *General Report 2006.*

ENISA, *General Report 2007.*

ENISA, *General Report 2011.*

ENISA, *General Report 2013.*

ENISA, *Annual Activity Report 2017.*

ENISA, *Press release* 2014. https://www.enisa.europa.eu/news/enisa-news/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol

ENISA, *ENISA Cyber security studies widely cited by OSCE* https://www.enisa.europa.eu/news/enisa-news/enisa-cyber-security-studies-widely-cited-by-osce.

ENISA, *Green light for new regulation for EU cybersecurity Agency ENISA given by the European Parliament* https://www.enisa.europa.eu/news/enisa-news/green-light-for-new-regulation-for-eu-cyber-security-agency-enisa-given-by-the-european-parliament.

European Parliament (2019)0151, *EU Cybersecurity Act*.