AALBORG UNIVERSITET

CYBERSPACE: OPPORTUNITY OR THREAT?

An analysis of the European Union's cyberspace policy based on its policy documents on cyberspace governance in the period 2010-2013 with the aim of determining how the EU has perceived and acted towards the emergence cyberspace.

20. DECEMBER 2016

AALBORG UNIVERSITET
Msc. European Studies
Anders Erik Thrige Nielsen

Keystrokes: 108988

Anders Erik Thrige Nielsen
European Studies
Master Thesis

Abstract

The emergence of cyberspace and ITC has ushered in the digital age. The digital age has resulted in positive as well as negative consequences for all actors inside and outside the cyber domain. It has empowered individuals around the world and helped revolutions on its way as seen with the Arab Spring. It has driven economic growth and created new markets. However, increase in cyber crime and major cyber attacks in Estonia 2007, Georgia 2008 and Iran 2010 along with cases of cyber espionage revealed in 2013, has all shown that serious risks and threats are evolving with cyberspace. Due to the rise of cyber incidents along with increased concern over critical infrastructure reliability of cyberspace many nation states are considering cyberspace the greatest security challenges of this century.

Regardless of the effects cyberspace has had on the world the amount of international relations research literature on the area is limited and in particular on the EU and cyberspace. Nevertheless, EU has an interesting role to play in regards to cyberspace because of its intergovernmental character, it is placed between the Member States and can play a facilitating and coordinating role. Which is important due to the borderless nature of cyberspace that is resulting in many cross-border issues. Due to this fact, this thesis is investigating how the EU has perceived the emergence of cyberspace and more specifically how the EU has presented its policy towards cyberspace in its policy documents in the period 2010-2013 and if any changes in the understanding of cyberspace can be located. Additionally, it is also studied how the EU's policy followed some of the general paradigms of understanding cyberspace with the aim of giving a deeper understanding on how the EU has perceived the emergence of cyberspace.

Three paradigms were constructed through reading in the research literature, media and reports. (1) social/economic paradigm, (2) political/ideologic paradigm and (3) security paradigm. The social/economic paradigm mainly focuses on cyberspace as a tool to affect the economy or society and is primarily optimistic about the effects of cyberspace. The political/ideologic paradigm mainly focuses on cyberspace as a communications tool that can spread ideas, values and norms. Security paradigm mostly focuses on cyberspace as a threat and a future battleground. These paradigms present different way actors understand cyberspace, however not one is dominant, and all paradigm recognises opportunities and threats in cyberspace.

Three EU policy documents are analysed: Digital Agenda for Europe (2010), The EU Cybersecurity Strategy (2013) and the NIS Directive (2013). The results found that, the EU's policy approach towards cyberspace in the period 2010-2013 has changed. The change was from a positive perception of cyberspace focused on exploding ICT's in the DAE to one more focused on security and limiting the threats and risks from the domain in the Cybersecurity Strategy and NIS Directive. Regardless, it was found that the EU followed the ideas of the social/economic and political/ideologic paradigms. This fact indicates that the EU's goal still is to profit from the opportunities inherited in cyberspace.

List of abbreviations

ASEAN	Association of Southeast Asian Nations
CERT	Computer Emergency Response Team
DAE	Digital Agenda for Europe (Commission Communication)
EU	European Union
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IGF	Internet Governance Forum
IoT	Internet of Things
IR	International Relations
NATO	North Atlantic Treaty Organization
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Co-operation in Europe
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
US	United States

Contents

Abstract i

List of abbreviations ii

1.0 Introduction: 2

1.2 Problem Formulation 3

2.0 Methodology 5

2.1 Literature review 5

2.2 Paradigms 8

2.2.1 The Social/Economic paradigm: 9

2.2.2 Political/ideologic paradigm: 9

2.2.3 Security Paradigm: 10

2.3 Approach 10

3.0 Analysis of the EU’s Policy Documents 13

3.1 Analysis a Digital Agenda for Europe 13

3.2 Analysis of the EU Cybersecurity Strategy 21

3.3 Analysis of the Network and Information Security Directive 29

4.0 Discussion 36

5.0 Conclusion 40

6.0 Perspectivation 42

7.0 Bibliography 44

1.0 Introduction:

Mobile devices, computers and the internet have become an integrated part of our society and our daily lives. These information- and communication technologies (ICT's) are affecting the way we communicate, trade, handle our economy and conduct politics (Christou 2016, p. ix). There has been a significant amount of benefits from the integration of ICT's into our society. Among the benefits are the empowerment the individual through access to easy and fast information and communication or the economic gain by reinforcing the existing marked as well as creating a new marked for IT-firms and related businesses (Kremer and Müller 2014, p. 42). Yet, the emergence of cyberspace has also been followed by an increase of threats and risk due to the emergence of this new electronic domain, which is often called cyberspace. The amount of systems and networks, (financial systems, voting systems, utility systems and so forth) which are connected and dependent on cyberspace are increasing. Due to these systems dependency, the effects of a cyber attack could in the worst-case scenario be catastrophic. Maybe for this reason managing cyberspace has been named one of the greatest security challenges of the 21st century (Sliwinski 2014, p. 468; Dunn Cavelty 2013, p. 3).

Even though that cyberspace policy and in particular cyber security policy has become an important policy issue that states cannot ignore it is worth noting that cyberspace and the internet are relatively new. The term cyberspace was invented by a science fiction writer named William Gibson in his famous sci-fi novel Neuromancer from 1984 and has since caught on as a term for describing computer- and information networks and maybe most often the internet. This short definition of cyberspace will be the basis of the project understanding term, meaning that cyberspace will include ICT such as the internet and computers, but could also refer to the domain in itself like other domains such as airspace (Kuehl 2009, p. 30).

Furthermore, the history of the internet goes back to 1969 when it was first developed in the United States (US) and used by the Defence Department as a communications tool. It was later made available to the public in the late 1980s with approximately 50 websites online (Ney 2010, pp. 2-3). By 2014 this number has grown to over 1 billion websites, and over 3 billion users worldwide and this number is increasing fast (Internetlivestats.com 2016, n.p.). Cyberspace is evolving, and it is getting bigger every day as more computers, technologies and individuals log on. Meaning that its influence on the world is increasing day by day.

However, with more people and technologies going online the risks and threats from cyberspace has grown with it. There have been serious cyber attacks in Estonia 2007, Georgia 2008 and Iran 2010 (Stuxnet worm) - just to name a few. Massive cyber espionage as revealed by Edward Snowden in 2013 along with an increase in cybercrime, which is getting more sophisticated every year. It can be said about all these threats that they are becoming more regular and costlier for the society (Dunn Cavelty 2013, p. 3; Christou 2016, pp. xi, 50). According to McAfee the cost of cybercrime globally was between $300 billion - $1 trillion in 2013 due to lost intellectual property (McAfee 2013, p. 5). Furthermore, one estimation calculates that the cost could reach $2 trillion by 2019 (Morgan 2016, n.p). These numbers should be taken lightly. First of all, the firms making these reports are often selling antivirus software and thus have an interest in inflated numbers. Additionally, determining the cost of stolen intellectual property is also highly subjective (Maass and Rajagopalan 2012, n.p.) Nevertheless, nearly 19 million websites were hacked in 2016 (Internetlivestats.com, 2016, n.p.) The amount of cyber attacks in 2016 shows that regardless of whether the costs are inflated, there is still a serious issue that needs to be handled or it can affect the economy and society.

The threats along with the benefits from cyberspace have resulted in the fact that cyberspaces have moved from low politics to high politics. High politics are involved with national security, essential institutions and decision systems that are considered critical to the state (Choucri and Clark 2012, p. 2). This shows how serious states have taken the emergence of cyberspace. However, it is not only nation states that have moved to influence cyberspace also international organisations such as UN, NATO, and EU have created policies on the cyberspace area. This project will investigate how the EU has perceived the emergence of cyberspace and how it has formed its policy approach towards it. However, what role can the EU play when security is a large part of the policies produced in regards to cyberspace? The EU can play a significant role in coordinating efforts along a facilitating role across the Member States (Christou 2016, p. 6). This role is critical because of the borderless characteristic of cyberspace (Lewis 2014, p. 2) leading to many cross-border incidents. It is in this regard that the EU intergovernmental (Sliwinski 2014, p. 469) character can play a important role, and it is, therefore, interesting to investigate the EU's policy approach towards cyberspace

1.2 Problem Formulation

At this point in history, we are at the beginning of the possibilities and capabilities of ICTs and still trying to understand how these new technologies will affect the way people conduct their everyday life. This is what is fascinating about cyberspace it is still developing, and scholars are still trying to understand the consequences of this process. Cyberspace is a new environment; a man-made environment and environment humans can change to its needs and liking (Demchak and Dombrowski 2011, p. 4). This is what makes cyberspace so unique it is simply new and never seen before. There is a need to create to investigate the consequences of the emergence of cyberspace, and international relations has a role to play in this objective.

Even though international relations can play a vital part in understanding the emergence of cyberspace by e.g. investigating the consequences of cyberspace on our society; which areas should be addressed politically; or the implication on national security. The amount of research literature on cyber IR is relatively limited, and this has also been observed by several scholars (Reardon and Choucri 2012, p. 2 Sliwinski 2014, p. 468; Eun and Aßmann 2015, p. 14; Christou 2016, p.12). Furthermore, both Sliwinski (2014) and Christou (2016) states that the research conducted on the EU and cyberspace is even more limited (p. 468; p.12). This fact also means that there is a lot of uncertainties and basics that need to be addressed before some of the more complex questions can be answered. This project will address the basics in the hope that others can use the results to solve the bigger questions.

Due to this fact, it has been found relevant to investigate how the EU has perceived the emergence of cyberspace and how this understanding has affected its policy approach. This will be done by analysing some of its policy documents and juxtapose with existing understandings of cyberspace or as they will be called in this thesis paradigms. The aim of this approach is to put the results into perspective and give a deeper understanding of the EU's policy and how the EU has reacted towards the emergence of cyberspace. These thoughts have led to the following problem formulation:

- *How does the European Union present its policy towards cyberspace in their policy documents in the period 2010-2013 and has the policy changed? Additionally, how does the European Union's policy follow some of the general paradigms of understanding cyberspace and what does that tell about the European Union's perception of the emergence of cyberspace?*

To clarity a paradigm will be understood as a collection of beliefs, values, norms, method and so forth used by a community of people e.g. scientist and politicians. However a more detailed explanation of the term is given in section 2.2. Due to the focus on how the EU has presented its policy towards cyberspace along with the definition of paradigms with highlights the importance of values and norms it has been found relevant to use Social Constructivism as the theoretical background for this project. A more detailed explanation for this choice is found in section 2.3.

2.0 Methodology

2.1 Literature review

The following section will present the important literature and scholars who have worked with cyberspace in a perspective of international relations. The literature that will be presented is the work of Johan Eriksson and Giampiero Giacomello (2010), Alexander Klimburg and Heli Tirmaa-Klaar (2011), Robert Reardon and Nazli Choucri (2012) Myriam Dunn Cavelty (2013), Krzysztof Feliks Sliwinski (2014) and lastly George Christou (2016). These scholars have been chosen on the criteria of the importance it has played on the scientific field as well as in the forming of this project.

Before the review of the literature is presented some general observation on research and cyber international relations must be addressed. It has already been stated that the amount of research on cyberspace from an international relation perspective is limited. Furthermore, there is even less research in regards to the EU and cyberspace because the literature has been focus on large cyber actors such as the US (Christou 2016, p. 12; Sliwinski 2014, p. 468). Hence there is a need for more research in general but especially in regards to the EU and cyberspace. Due to this fact, it has been found relevant to present central research on the EU and cyberspace to highlight which aspects has been researched.

The literature by Klimburg and Tirmaa-Klaar (2011), Dunn Cavelty (2013), Sliwinski (2014) and Christou (2016) are all working with the EU and cyberspace. Even though they all investigation different aspects of the EU policy towards cyberspace there is still a general theme of focusing on security. Klimburg and Tirmaa-Klaar's paper is studying the problems related to cybersecurity and cyberwar on the EU's foreign policy. Dunn Cavelty is investigation the EU's Cybersecurity Strategy with the use of the Copenhagen School and securitization. Sliwinski's research is focusing on the EU as a cyber security actor and applies intergovenmetalism. Lastly, Christou is investigating the EU's approach to internet governance and cyber security by applying a more pragmatic approach where he *"(…) draws on existing theorisations of cyber security more broadly"* (Christou 2016, p.11). Hence it is clear that the focus of research conducted on cyber IR and the EU has had a focus on the security aspect of cyberspace. These works are relevant and give excellent contextual insight on the EU and cyberspace. However, what can be seen above is that the researches has been relatively one-sided in their research approach. Therefore has this project taken a broader perspective by investigation the EU's perception of cyberspace and how this has affected its policy approach. This does not mean that security is excluded, but rather that other aspects are also found relevant.

Klimburg and Tirmaa-Klaar's work provides valuable insight into the aspects and definitions of cyberpower and cyber warfare. Furthermore, they also present short reviews of China, Russia, and the US policies towards cyberspace. Lastly, it investigates the EU's approach towards cyber security until 2011 and gives assessments for action that can boost the EU's cyberpower in the future. One of the major conclusions is that liberal democracies are at a disadvantage because governments have limited control over cyberspace since non-state actors are responsible for the daily function of it. The democracies must convince the non-state actors to adopt effective cybersecurity measures, where other more authoritarian states have a better ability to co-opt or coerce the non-state actors and thereby giving them an advantage in building a more secure national cyberspace (Klimburg and Tirmaa-Klaar 2011, pp. 14-19). Klimburg and Tirmaa-Klaar conclude that the EU's approach has been fragmented yet the actions taken by the EU has helped to build more resilience in the Union (Klimburg and Tirmaa-Klaar 2011, pp. 29-42). The research is relevant but has a limited focus on cyber security and do not present a more general presentation of the EU's policy actions taken towards cyberspace.

Dunn Cavelty's paper on the EU's Cybersecurity Strategy from 2013 does not only give an insight into the policy document but also the EU's past actions in the area as well as the development of cyberspace governance. The principal conclusions of Dunn Cavelty's work are that the open and free internet is under attack and it is not only from totalitarian states but also democracies. Due to this fact, Dunn Cavelty concludes that EU must stick to its policy of supporting an open and free internet and through this, it can become a powerful international cyber security actor (Dunn Cavelty 2013, p. 11). However, Dunn Cavelty never explains why the EU should or must support the open and free internet. Additionally, she does not investigate if the EU could possibly change its policy approach. The point here is that Dunn Cavelty is locked in the perspective that considers the current open configuration of cyberspace is the best or only option.

Sliwinski's article gives an updated insight into the development of the EU's action in regards to cyberspace and shows some of the limitation that the EU faces because of its intergovernmental character. Sliwinski's concludes that the EU's effectiveness as a cyber actor is restricted by a fragmented vision on cybersecurity among the Member States. Furthermore, Sliwinski states that the EU's understanding of cyberspace as a trading platform or communications tool will hinder its ability to play a significant role in the policy area. Sliwinski lastly concludes that the EU needs to adopt different forms of cyber power and that a simple defensive approach will not be enough to affect the vast number of cyber actors and in general cyberspace (Sliwinski 2014, pp. 468-481). However, Sliwinski never really explains how the EU should move from a defensive approach to a more offensive one – which arguably is an interesting question.

Christou's book is the most comprehensive work to date on the EU and cyber security. Due to this fact, it has played a significant role in forming this project. The book gives an excellent contextual understanding of the EU and its actions towards cyberspace as well as prediction of its future development. One of the major conclusion by Christou is that the EU's current policy on resilience building is the best method to create security. To build resilience in the EU Christou identifies the need for trust building and that the approach should be based on the multi-stakeholder model (Christou 2016).

Furthermore, Christou notices that amount of theoretically informed work on cyber security is limited (Christou 2016, p. 12). It is in this regard that Eriksson and Giacomello plays an important role. Eriksson and Giacomello have in their work on international relations and security in the digital age looked at the gap between IR theory and research on cyberspace. They found that realism has issues with handling cyberspace especially due to their state-centric understanding. This is an issue since ICT's has given non-state actors more power. For the same reason, liberalism and constructivism have a bigger role to play because they can take multipolarity of actors into account. The conclusion is that a more pragmatic approach towards studying cyberspace is needed as well as the need to develop a middle-ranged theory (Eriksson and Giacomello 2010, pp.1-28). In the research conducted by Reardon and Choucri, it was also found that constructivism was the most applied theory to analyse cyberspace with (Reardon and Choucri 2012, p. 6). This gives further merit to the applicability of the constructivist theory on cyberspace.

The short presentation of the research on the EU and its cyberspace policies has clearly shown that the dominating approach towards the subject area is based around cyber security. The focus on security is not uncommon in research on cyber IR as Reardon and Choucri explain in their paper from 2012. Reardon and Choucri's paper reviews the literature on cyberspace and IR over the previous decade. Their findings show that the dominating theme in the literature has been on security. However, four other themes are presented: global civil society, governance, economic development and cyberspaces effects on totalitarian states (Reardon and Choucri 2012, p. 1-29). Reardon and Choucri's article gives an interesting insight the literature on the subject area and helps to get an understanding of some of the paradigms located in the research literature in general. Therefore, it has also assisted in the construction of the next section on paradigms.

2.2 Paradigms

This section will present what is understood as a paradigm in this project. Furthermore, three paradigms in regards to how cyberspace is understood have been constructed by using observation from the existing literature on the field along with reports, media and more. This section will present these paradigms and their characteristics.

First, an understanding of the term paradigm, as well as the definition used in this project, must be given. The term paradigm and its meaning in science were coined by Thomas Kuhn in 1962 in his book 'The Structure of Scientific Revolution'. Kuhn defines a paradigm as being based on two characteristics: (1) An achievement which is so unprecedented that a group of people steers away from the opposing methods. (2) the achievement must be so open ended that it leaves enough unanswered questions and problems which the group can solve. (Kuhn, 1970, p. 10). By achievement Kuhn refers to scientific theories such as Newton's laws. His theory had the two characteristics presented above and changed the scientific method used by the physicist in the period thereby creating a new paradigm. This understanding of a paradigm is not entirely applicable to this project however, as explained by Christopher G. A. Bryant (1975) Kuhn later stated that *"(...) in a general sense, a paradigm is an 'entire constellation of beliefs, values, techniques, and so on shared by members of a given community' (...)"* (Bryant 1975, p. 354). It is this definition that will be used to describe paradigms in this project. Additionally, it must be stated that Kuhn explains that a paradigm is often accepted by the whole field because it is successful in answering some critical question shared by the community (Kuhn 1970, p. 23). Since cyberspace is still relatively new, the consequences and effect on the world are not fully grasped. For the same reason, no single paradigm has been accepted as explaining the effects of ICT and cyberspace. However, through reading IR research on the field, reports, and media three competing paradigms has been located: (1) Social/Economic paradigm, (2) Political/Ideologic paradigm and (3) Security Paradigm. The paradigms represent three ways that different groups perceive the emergence of cyberspace. However, this does not mean that they do not acknowledge the other paradigms, yet the group/community still has a focus on one of the presented paradigms.

Before identifying the characteristics of the three paradigms it must be stated that there are no direct references to the paradigms in the literature, media or policy documents. These are based on observation on how different actors approach cyberspace through the way they talk and write about the subject area. Furthermore, as with the observation from the introduction – that cyberspace both encompasses opportunities as well as threats – the same can be seen in the three paradigms where both positive and negative consequences are recognized. Yet there still is a tendency of the actors to favour either a positive or negative perception. By locating which of the three paradigms' the EU favours in its policy documents as well as whether they see opportunities or threats will help to identify the EU's policy towards cyberspace. Furthermore, by applying this method to the individual policy documents it is possible to determine possible changes in the EU perception through the period 2010-2013.

2.2.1 The Social/Economic paradigm:

This paradigm is based on idea that cyberspace mainly will affects the society and the economy and that cyberspace is primarily understood as a possibility to create a new economy (Lotrionte and Maurer 2012, p. 2) which in the media often is presented under terms such as Internet of Things (IoT) or Industrial Revolution 4.0. Terms that highlighting the significant that cyberspace will have on the industry and economy. This economic optimism is also presented in Reardon and Chourcri article where one of the themes is 'economic development'. The research literature has here mostly been focused on the promised effects that ICT will have on the economy and society by creating growth through easy access and sharing of information (Readon and Choucri 2012, pp. 14-16). However, some negative consequences of this development are still acknowledge. One example is the 'digital divide' which refers to fact that ICTs likely will create and deepen the differences between developed societies and third world countries. Some predict that this divide could result in security issues because the poor countries will turn violent to get some of the gain (Readon and Choucri 2012, p. 15).

2.2.2 Political/ideologic paradigm:

This paradigm is based on the idea that cyberspace mainly is used to forward political means and ideologic values. This paradigm mostly focuses on cyberspace and ICTs as a communications tool that brings down barriers between societies and can be used to spread ideas that can change identities and perceptions (Reardon and Choucri 2012, p. 22). This paradigm can be seen in Reardon and Choucri's identified themes 'global and civil society' where cyberspace's ability to promote democratic reform and values through cyberspace is explained. For this reason, cyberspace is also perceived as a threat by totalitarian states that fears the open and free characteristics of cyberspace (Reardon and Choucri 2012 pp. 8-11). Another aspect of this paradigm is that it can also be used by terrorist organisations as a propaganda tool or for recruitment purposes which as least from a western standpoint has been view with increased concern - so much that some perceive cyber terrorism as a greater threat than cyber attacks against critical infrastructure (Reardon and Choucri 2012 p. 23).

2.2.3 Security Paradigm:

In this paradigm it is argued that cyberspace mainly or at least foremost should be perceived as a threat to society, the economy or in other words as an existential threat to the nations. Therefore, under this paradigm cyberspace is primarily perceived as a possible battleground for future wars and that cyberspace is a weapon that needs to be built security against. Cyberspaces is perceived as a threat due to *"The low price of entry, anonymity and asymmetries in vulnerability (…)"* (Nye 2010, p. 1). These characteristics has created more vulnerabilities and multiple angles of attack. These attacks can come from a small actor (individual in a garage) or a large nation (China) yet no sufficient way of identifying who is behind it. This understanding along with the concerns that a cyber attack against critical infrastructure could have devastating effect on the society has created a fear for the future in the digital age. This idea is also known under the populistic term 'cyber Pearl Harbor' which draw on the idea of a doomsday scenario (Eun and Aßmann 2015, p. 2). The benefits of cyberspace and ICTs are recognized however, the focus is on the threats and how to protect against them. Terms such as cyber war, cyberpower and cyber warfare is commonly used. (Reardon and Choucri 2012 p. 22; Klimburg and Tirmaa-Klarr 2011, pp. 5-20)

With a definition of how paradigms are understood in this project along with an explanation of the three identified paradigms on how cyberspace can be perceived by different actors, the approach used towards answering the problem formulation can be presented.

2.3 Approach

Due to the nature of the research question as well as the definition used to explain paradigm in the project the theoretical basis for this project is Social Constructivism or simply constructivism. The argument behind this is because *"A fundamental principle of constructivist social theory is that people act towards object, including other actors, on the basis of the meanings that the objects have for them."* (Wendt 1992, pp. 396-397). With a focus on how the EU has presented its policy towards cyberspace as well as an understanding of paradigms that emphasises values, interests, and norms, it can be argued that constructivism is the obvious choice. Constructivism often uses 'speech acts' to determine how an actor perceives an object because constructivist believe that how an actor talk about an object indicated how the actor thinks about it (Eriksson and Giacomello 2010, p. 19). This perception is e.g. seen in the way constructivist believe that policy is constructed, developed, perceived and communicated using language (Christou et. al 2010, p. 346). This means that by analysing how an actor talks about and object we can determine the meaning the actor gives it and thereby explain and understand how they have acted. Due to this fact, constructivism has been found relevant as a theoretical background for this project. So, with the paradigms sorted and a theoretical background for the analysis presented it is now possible to demonstrate the structure of the analysis and how the research question will be answered. here

Each analysis will be focused around how the EU presents its policy in the selected policy documents. Each analysis will start with a short presentation of the main actions and goals of the policy document. This will be followed by an analysis of how the EU presents its policy towards social and economic aspects, political and ideologic aspects and lastly security aspects. By aspects, it means how the EU writes about these areas, what they highlight, and what that tells about the EU's policy. This approach has been chosen because it is believed that this will highlight the EU's policy towards the subject area as well as create a good foundation to discuss whether any of the identified paradigms is present in the policy documents. Each analysis will be concluded with at summary discussing the findings and whether the policy documents has a dominating paradigm. The aim of this approach is to put the findings into perspective as well as getting a deeper understanding of the subject area because each paradigm presents different understandings of the opportunities and threats inherited with cyberspace.

The analysis will be followed by a discussion that collects the findings of the analysis and forms an answer to this project's research question. After the discussion, the conclusion of the project is given. This section will present the results of the project and answers the problem formulation. Lastly, the project will be ended with at perspectivation. This has been found relevant due to the general need for more IR research on cyberspace. Therefore, the perspectivation will be centred around possible future research.

However, before the analysis can be conducted some limitations needs to be set. Three policy documents produced by the EU will be analysed: **(1)** *The European Commissions: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe (2010).* **(2)** *The European Commissions: Joint Communication to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions – Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013)* and lastly **(3)** *the European Commissions: Proposal for a Directive of the European Parliament and of the Council – Concerning measures to ensure a high common level of Network and Information Security across the Union (2013).* It is worth noting that more policy documents from the selected period which directly or indirectly addresses issues related to cyberspace could be located. However, these policy documents have been selected because they are some of the most comprehensive policy documents produced by the EU directly addressing cyberspace. Furthermore, these documents have also been analysed by the presented scholars in the literature review, which gives the possibility to juxtapose the results from this project with the presented literature. Additionally, it is believed that these three documents will provide enough empirical data to answer the problem formulation of this project, but it is not given that this will represent the full picture of actions taken by the EU in regards to the emergence of cyberspace.

Another limitation is the selected period which is analysed. The period that has been chosen is from 2010-2013. The reason behind this period is that several major cyber events happened in the period before 2010 such as the cyber attacks against Estonia in 2007 or Georgia in 2008. The reason behind picking 2010 instead of 2007 is due to that fact that these cyber events showed the dangers lurking in cyberspace and made cybersecurity *"(...) the policy-issue of the hour."* (Dunn Cavelty 2013, p. 3). The attacks resulted in an increased focus on the area from the Commission which stated to produce regulations and directive to address cyberspace (Dunn Cavelty 2013, p. 4). The presented policy documents above are a result of this effort and therefore sets a natural, historical limit to this project. The reason behind ending the project in 2013 lies in the fact that the documents were published in 2013. To this, it is worth mentioning that they both were concluded in 2016, but since the papers and documents of the negotiations is not taken into consideration in the analysis the period was limited to the year the policy documents was published.

The last aspect there needs to be addressed is the European Union. The author of this thesis acknowledges the special nature of the EU as an intergovernmental institution (Sliwinski 2014, p. 469). However, this project will see the documents as a representation of the collective understanding of cyberspace shared by the EU. However, it is recognised that different institutions and agencies inside the EU, as well as the Member States, does not necessarily share the vision of the drafters of the selected documents. However, it is still believed that the findings and the documents represent the general perception on cyberspace inside the EU.

3.0 Analysis of the EU's Policy Documents

With an understanding of three identified paradigms along with the approach, limitations and definitions it is now possible to analyse the selected policy documents. The following chapter will investigate EU's policy documents with the aim of answering this thesis's research question.

3.1 Analysis a Digital Agenda for Europe

This section is an analysis of the *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe.* The first part of the analysis will be a short review of the content of the policy document. Subsequently the analysis of how the EU has presented its policy towards social/economic aspects, political/ideologic aspects and security aspects of cyberspace will be given. The analysis will be divided in three sections that each focuses on one of the presented aspects and whether any of the presented paradigms is followed. Lastly, a short discussion will be conducted to determine the dominating paradigm if any in the Communication.

The Digital Agenda for Europe Introduction

On May 19, 2010, the Commission published the policy document: A Digital Agenda for Europe commonly referred to as the DAE. The Digital Agenda is one of seven initiatives leading from the Europe 2020 strategy which aims it is to get Europe out of the crisis and prepare the EU's economy for the next decade (European Commission[b] 2016, n.p.). Due to the DAE being a communication it does not hold any mandatory authority meaning that the policy document does not have any legal effect and only highlight the Commissions thinking on the issue (European Judicial Network 2016, n.p.). The Directorate-General for the Information Society and Media was the leading service in the drafting of the policy document. Furthermore, the Communication has been subjected to debate both in the Council of the European Union, the European Parliament as well as the Committee of the Regions and the Economic and Social Committee. The DAE was concluded by the Council on May 28, 2015.

The Communication identifies seven obstacles that limit the EU's benefits from ICT: (1) *Fragmented digital markets,* (2) *lack of interoperability,* (3) *rising cybercrime and risk of low trust in networks,* (4) *lack of investment in networks,* (5) *insufficient research and innovation efforts,* (6) *lack of digital literacy and skills and* (7) *missed opportunities in addressing societal challenges*. (European Commission 2010, pp 5-6). The aim of the DAE is to present an action plan to tackle these seven sets of obstacles before 2020 and *"(...) deliver sustainable economic and social benefits from a digital single market (...)"* (European Commission 2010, pp. 3, 5-6).

To obtain the goals of the DAE the EU propose seven action points: (1) *a vibrant digital single market,* (2) *interoperability and standards,* (3) *trust and security,* (4) *fast and ultra fast internet access,* (5) *research and innovation,* (6) *enhancing digital literacy, skills and inclusion and (7) ICT-enabled benefits for EU society.* By implementing these seven actions, the EU hope to take full advantage of the potential of ICTs in resolving economic and social problems. (European Commission 2010, pp. 3, 6-33).

The last part of the policy document focuses on international cooperation. In the DAE this is not a part of the seven initiatives. However, the EU acknowledges that to solve the identified obstacles international cooperation is needed since, as the EU explains it, all the action areas have an international dimension. Therefore, the last 'action area' is to promote the internationalisation of internet governance built on a multi-stakeholder model. (European Commission 2010, pp. 34-35)

With the short presentation of the content and aim of the DAE, the analysis of the EU policy approach can be conducted. The following section will analyse the social/economic aspects of the DAE and how the EU perceives the emergence of cyberspace in an economic and social perspective. Furthermore, the findings will be put into perspective of the social/economic paradigm. The same method will afterwards be done with political/ideologic aspects and lastly with the security aspects.

The DAE on Social and Economic Aspects

In the content presentation above there are indications that the DAE has a high economic and social focus, this is further supported by the fact that the aim of the policy documents is to make sure that the economic and social benefits of a single digital market becomes a reality. Thereby already indication that the social/economic paradigm is present in the DAE.

In regards to the social/economic aspects, one of the first interesting observation is that the EU does not use the term cyberspace in the document but rather internet or ICTs. This lack of use could indicate that there is an attempt to stay clear of the term maybe because it is too unclear for the EU drafters and their policy documents. Instead, they use the term ICT which is a more precise term and goes beyond the internet – which cyberspace is often only associated with. On the other hand, the policy document also shows that the EU is mainly focusing on the internet by stating that among the ICT the internet has become *"(...) an integral part of daily life for many Europeans."* (European Commission 2010, p. 24) and that *"The internet has now become such a critical information infrastructure for individuals as much as for the European economy at large (...)"* (European Commission 2010, p. 6). This quote clearly puts the internet as the most important technology of the ICTs in the DAE and highlights that the EU understand that the internet has had an importance impact on society. Furthermore, what can also be seen in the last example is the fact that the EU identify the internet and ICTs as an import part of the economy. To this, the EU later add that *"ICT drives value creation and growth across the economy."* (European Commission 2010, p. 23). These examples show that the EU perceive cyberspace and ICT's to have a positive effect on the economy. Additionally, it is worth noting that the way EU write about it could suggest that they do not only perceive the positive effect is in relation to economy regarding online sales, phone market, computer sales and so forth, but that it also influences and enables other parts of the economy to grow. This suggest that the EU perceives the internet and ICTs as an economic tool to get itself out of the crisis – which also is the aim of the DAE and the Europe 2020 strategy (European Commission 2010, p. 3)

Another interesting aspect that can highlight how the EU perceives the social/economic effects of ICT is how the EU envision the future of the internet and how the digital age will affect the world. Furthermore, by investigating this aspect an understanding of whether the EU sees possibilities or threats lurking in the future can be given. In this regard, the EU predicts that the future economy will be knowledge based and centred on the internet and the EU, therefore, view digital competences to be fundamental for the EU citizens in the future (European Commission 2010, pp. 19, 25). This understanding does support that the EU view the internet as the primary ICT and it also supports the argument that they see it as a valuable economic tool since it will play a central role in the future economy. The fact that the EU believes in the ability of cyberspace to drive economic growth further supports the claim that the EU's policy in the DAE follows the social/economic paradigm.

The section above also indicates that the EU perceives this as an area of vital importance and if the EU lacks behind in innovation and education of IT talent, it will not be able to keep its competitive edge (European Commission 2010, p. 22). This fact is also visible in the way the EU compares itself to competing economies in the DAE. The comparisons show how the EU lacks behind in downloading music (sales online), fibre connections and R&D spending. That the EU is comparing itself shows a concern and that they see the possibility of adverse effects if the EU is not competitive in the ICT area compared to other nations such as the US and Japan. The fact that the EU shows concern about the future highlights that the EU does not perceive all aspects of the emergence of cyberspace as positive – at least if the EU does not act accordingly and minimise the negative effects. Nevertheless, the EU is still more focused on the positive outcomes which are best shown by this quote: *”The Digital society must be envisioned as a society with better outcomes for all.”* (European Commission 2010, p. 27)

The section above shows how the EU wants the future in the digital age to look like and how it can look if they harness the transformative power of ICTs. So even though ICTs can be a threat in the future, it will only be so if the EU does not grasp the opportunities it brings both for the economy and for the society. This understanding is further shown here: *“But while the transformational power of ICT is clear, serious challenges must also be confronted in order to harness it.”* (European Commission 2010, pp. 4-5). This quote supports the argument above and clearly shows that the EU does not ignore that there is a risk involved with the ICTs. These findings support that the EU subscribes to some of the beliefs of the social/economic paradigm especially in regards to cyberspace and its ability to transform and empower the society and economy. Furthermore, even though concern can be spotted, the tendency in regards to describing social and economic aspects of the policy shows more optimism than concern. This argument further supports that the EU follows the ideas from the social/economic paradigm in the DAE.

The DAE on Political and Ideologic Aspects

A political/ideologic aspect that tells a lot about the EU’s policy approach towards cyberspace is in the way the DAE describes the internet as open, neutral and borderless (European Commission 2010, pp. 5, 7, 20). This understanding is however not shared by all actors in cyberspace. The reason lies in the fact that the internet promotes liberalisation, democracy along with freedom of speech, information and communication. (Deibert 200, p. 501). As already explain it is especially totalitarian states which are moving for more control over the internet. However, recent years have shown that also democratic states have acted to limited the freedom and openness of the internet to gain more security (Dunn Cavelty 2013, pp. 7, 11). By defining the internet as being open and neutral, the EU shows its commitment to keeping the internet at a status quo that is based on limited governance and government involvement (Klimburg and Tirmaa-Klarr 2011, p. 20). That the EU supports the open and free nature of cyberspace is maybe most clear in the following citation:

"Europe must continue to play a leading role (...) in promoting a governance of the internet as open and inclusive as possible. (...) It is a formidable instrument for freedom of speech worldwide" (European Commission 2010, p. 34).

This open and free characteristic of cyberspace and its effects has been one of the main focuses of the research literature as shown by Reardon and Choucri (2012, pp. 8, 17). When the EU describes the idea of the internet to be open and free, they follow the concept of the political/ideologic paradigm. This could suggest that the EU perceives the internet as a communications tool to spread values, ideas and norms. Due to this fact, it is not farfetched that the EU wants to use the internet as a means to spread its political and democratic values through cyberspace. Thereby the EU's policy again focuses on the possibility of cyberspace in regard to be able to spread values rather than the possible threats that other actors, such as terrorist, can use the internet to spread propaganda.

The EU also makes it clear that it will promote the internationalisation of cyberspace but it must be based on the multi-stakeholder model. The multi-stakeholder model is where cyberspace governance is shared by governments, private cooperation's and the civil society in a bottom-up structure (Klimburg and Tirmaa-Klarr 2011, p. 22, Klimburg 2013, p. 2). The multi-stakeholder model is often considered *"(...) the bedrock of the free Internet (...)"* (Klimburg 2013, p. 2). Hence it plays a critical role in the keeping the open and free structure of cyberspace. Additionally, the EU makes it clear that it will support the Internet Governance Forum (IGF) beyond 2010 (European Commission 2010, p. 34). This should go to show that the EU want to protect the multi-stakeholder model as well as the open and free characteristics of the internet. However, as with the open and free structure of the internet the multi-stakeholder model is contested from multiple fronts and this can, therefore, be quite a challenge for the EU.

A question still stands, why does the EU so strongly support the idea of keeping cyberspace open and free? One reason is properly due to the EU's focus on liberal values. This argument is backed up by the fact that the EU's policy also has a strong focus on fundamental rights (European Commission 2010, pp. 5, 17). An important aspect of the fundamental rights is the freedom of speech but also privacy. Thereby the EU cannot support government surveillance, filtering or more government control because it will directly affect the EU's commitment to the fundamental rights as well the open and free nature of cyberspace. Additionally, the observation that the EU wants to use cyberspace as a tool to spreads its values and norms gives them further incentives to protect these aspects of the internet.

However, another argument for the EU's strong support for the open and free nature of cyberspace could be explained by the effect the EU predicts it will have on the economy. The DAE states that an open platform will help the to push innovation and development of new ICTs (European Commission 2010, pp. 20-21). With the knowledge that the EU's policy follows the line of the social/economic paradigm gives merit to this explanation. Due to this fact, it also supports the findings of the former section. However, this does not undermine that the other aspects also influence the EU's policy approach.

The DAE and Security Aspects

One way to get a clear understanding of how the DAE describes security aspects is by looking at how the EU defines cybersecurity. However, there is no direct definition of how cybersecurity is understood by the EU in the document. Yet, it is possible to get an insight into what they identify as threats from cyberspace as well as how they will handle these threats and why. However, the fact that no definition on cyber security is presented in the document gives the first hint to how the focus it has in the EU's policy in the DAE.

Security is a part of the seven action points of the DAE, and it is under the title: *Trust and Security*. This title shows in many ways how the EU view security in the DAE and that is that it is closely linked to creating trust in the systems and technologies. Due to this focus, another action point is also interesting, and that is point number 3. *Building digital confidence*. The reason these are somewhat linked is due to the EU understanding that: "*Europeans will not embrace technology they do not trust (…)"* (European Commission 2010, p. 16). To this the EU has observed that a lack of trust in the function of the internet is already having a negative effect on the digital economy and that *"Consumers will not* **shop online** *if they do not feel that their rights are clear and protected"* (European Commission 2010, p. 12). This is one of the key perception behind the EU's strategy towards security in the DAE – Security is needed to create trust, and with trust, the European citizens will embrace the ICTs and the internet. This indicates that security is a way to reach other goals – such as getting people to shop more online. This fact could suggest that the EU is more focused on the possibilities rather than the threats from cyberspace and therefore not share beliefs with the security paradigm.

In the seven obstacles presented in the content presentation, one of the barriers or threats that the EU faces is increased cybercrime. What the EU identifies as cybercrime is: Child abuse, spam emails, identity theft and cyber attacks which they say are mostly motived by financial purposes but also can have a political nature – which has been seen in Estonia, Lithuania and Georgia (European

Commission 2010, pp. 5, 16). In the DAE the EU does not use much time on the politically motivated attacks which could indicate that its primary concern is on the economic effect cyber attacks can have. Which again suggest that the EU is focusing on the economic aspects of cyberspace.

With an understanding of what threats and risks the EU have identified in the DAE, the next question is one how the EU will handle these threats. What is interesting is that for the EU states *"(...) the internet has proved remarkably secure, resilient and stable, but IT networks and end users' terminals remain vulnerable to a wide range of evolving threats (...)"* (European Commission 2010, p. 16). This understanding shows that the EU will not try to affect the functioning of the internet since they simply do not see any issue in the way it functions – quite the contrary. Thereby this also supports the recent argument that the EU wishes the internet to stay at a status quo of open and neutral. Due to this fact, the EU concentrates on two things in the DAE to create a secure cyberspace or digital environment and to protect the fundamental rights and privacy of people.

Despite the fact that the EU's policy is focused on the protection of fundamental rights and privacy it can still be argued to be surrounding the goal of creating trust in the system so that citizens will shop online and use ICTs. However, there is also an ideologic reasoning behind this focus, and that can be observed in this quote: *"The right to privacy and to the protection of personal data are fundamental rights in the EU which must be – also online – effectively enforced using the widest range of means".* (European Commission 2010, p. 17). The EU furthermore states that "(…) *the digital age is neither "big brother" nor "cyber wild west"."* (European Commission 2010, p. 16). By this, the EU clearly expresses that it envisions cyberspace without surveillance (which follows in line with the focus on privacy) and cyberspace as a secure place. The point here is that even though a strong focus on social and economic aspects is present, the other two aspects also plays a significant role in the EU's policy towards cyberspace. However, the findings still do not support that the EU's policy approach follows the lines of the security paradigm.

Summary

There is no significant focus on cyber security in the DAE and what is presented mainly focuses around trust-building which should be apparent in the documentation above. The focus on trust-building is however quite interesting and supports that the social/economic paradigm is dominating in the DAE. This indicates that the EU perceives that the threat and risk associated with cyberspace are technicalities that need to be handled. To this argument, it is relevant to notice that the United States already in 2009 marked cybersecurity as a high priority (The White House 2009) meaning that cybersecurity was already a serious issue which was handled by other nations which the EU compares itself to (as it also has done in the DAE). Therefore, it could be argued that the DAE could have had a far stronger focus on cyber security and seen this as an issue in its own right. What is apparent in the DAE is that the EU, of course, acknowledges the threat from cyberspace. However its policy is still centred around obstacles that need to be handled so the power of ICT can be harnessed to transform the EU society and economy with the overall aim of getting the EU out of the crisis. Due to the fact, that this understanding is so present in the documents, it is also argued that the dominating paradigm of the DAE is the social/economic paradigm.

The DAE and the strong presence of the social/economic paradigm could be argued to be a product of the time. It is written with a positive understanding of cyberspace or ICT as a tool which can be harnessed with the right actions to solve the EU's problems they had at that moment. However, with Europe gradually getting out of the crisis, cyber attacks against the EU institutions in 2011 and continued increase in cyber crime the EU's policy and understanding of cyberspace could have been affected by these events. That is what the next two chapters will consider when the EU's Cybersecurity Strategy and NIS Directive is analysed.

3.2 Analysis of the EU Cybersecurity Strategy

This section will analyse the content of the *Joint Communication to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.*[1] First, there will be a short presentation of the document followed by a brief review of the content of the policy document. The introduction will be followed by an analysis of how the EU presents its policy towards social and economic aspects of cyberspace. Then an analysis of respectively political/ideologic aspects and security aspects will be conducted. Lastly, the chapter will be finished with a short discussion to determine if one paradigm is dominant in the Communication.

Cybersecurity Strategy Introduction

On February 7, 2013, the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy published the Cybersecurity Strategy for the European Union. The policy document is a communication which again means that it does not have any mandatory authority. Due to it being a Joint Communication the leadings services behind the drafting of the document was Directorate-General for Communications Networks, Content and Technology; European External Action Service and the Directorate-General for Migration and Home Affairs. The document was sent to the Council of the European Union; Committee of the Regions; European Parliament; the European Economic and Social Committee. The Communication was concluded by the Council on the 9. June 2016.

The EU Cybersecurity Strategy highlights five strategic priorities that shall combat the issues emerging from cyberspace. *(1) Achieving cyber resilience, (2) Drastically reducing cybercrime, (3) Developing defence policy and capabilities related to the Common Security and Defence Policy (CSDP), (4) Develop the industrial and technological resources for cybersecurity and (5) Establish a coherent international cyberspace policy for the European Union and promote EU values* (European Commission[a] 2013, pp. 4-5). The aim of these priorities is to create *"(...) an online environment providing the highest possible freedom and security for the benefit of everyone."* (European Commission[a] 2013, p. 4)

[1] Will hereafter be referred to as the Cybersecurity Strategy.

The section above is the presentation of the five strategic points that the EU Cybersecurity Strategy highlights. With a basic understanding of the content and goal of the Cybersecurity Strategy, the analysis of the policy document can be conducted.

The EU's Cybersecurity Strategy on Social/Economic Aspects

In the Cybersecurity Strategy, the term cyberspace, which they for some reason left out of the DAE, is being used in the policy document. The EU states that: *"Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society"* (European Commission[a] 2013, p. 2). This quote shows that the EU still perceives cyberspace and in particular the internet to have a large impact on society. This follows the line of the social/economic paradigm as well as the understanding from the DAE. Since cyberspace has had such an effect on society, the EU makes it clear that ICT's needs to work seamlessly for the same reason (European Commission[a] 2013, p. 2). This understanding sets a new tone in the EU's policy towards cyberspace where security is more in focus.

However, the social/economic paradigm is still present, but the nearly utopian view on cyberspace from the DAE has changed to a more concerned view. This can e.g. be seen in this quote:

"Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the internet and the smooth functioning of information systems." (European Commission[a] 2013, p. 2)

This example shows that the EU still believe in cyberspace and ICTs ability to create growth by describing it as the backbone of the economy and through this the EU also highlights how critical they perceive this aspect. This fact suggests that the EU still firmly believe in cyberspace and its ability to create prosperity for the EU and thereby the policy approach still follows ideas from the social/economic paradigm. What the example also show is an increased concern about the increased reliance on ICTs in multiple sectors and here especially areas that are critical for the society and economy. In the DAE the EU was mainly concerned about not being competitive in regards to the IT market what the example shows is that the EU is getting more concerned about the consequences of a cyber attack and the adverse effect is will have - especially on the economy.

The EU however still believes that if they can create enough security they can harness the economic opportunities of cyberspace. This can be seen through the fact that the EU still wants to create a Digital Single Market which they believe *“could boost its GDP by almost €500 billion a year; an average of €1000 per person”* (European Commission[a] 2013, p. 2).

One aspect that the Cybersecurity does not refer to quite as much is the social aspect and the possibilities or challenges that cyberspace has on society. However, the protection of fundamental rights, privacy and the protection of personal data is still present and even more than in the DAE.

The Cybersecurity Strategy on Political/Ideologic Aspects

What can be seen from the last section above is an indication that the Cybersecurity Strategy is focusing on the political and ideologic aspects of cyberspace. One aspect that has caught the attention even more of the EU is cyberspaces ability to spread values and norms. This ability is one of the first aspects that the Cybersecurity Strategy highlights:

“An open and free cyberspace has promoted political and social inclusions worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies – most strikingly during the Arab Spring.” (European Commission[a] 2013, p. 2)

This example clearly shows the ideas of the political/ideologic paradigm and draw attention to how good a tool cyberspace is to spread liberal and democratic values. One reason for the increased focus on this ability can also be spotted in the example above. The reference of to the Arab Spring as an example of this ability is interesting, particularly with the knowledge that social media played a significant role in enabling the uprising (Reardon and Choucri 2012, p.19). This indicates that the Arab Spring has reinforced the EU's understanding of the abilities of ICT and how it can help to spread liberal ideas. Under the fifth strategic point (CFSP) the EU explains that the important priorities in its policy approach are to promote cyberspace as open and free and that expanding access to the internet should help to *“(...) advance democratic reform and its promotion worldwide.”* (European Commission[a] 2013, p. 15). This further confirms that the EU not only recognises that cyberspace can promote liberal and democratic values but that they wish to use it in its policy approach. To this it can be added that the EU perceives that the internet now has become *“(...) one of the most powerful instruments for global progress without governmental oversight or regulation.”* (European Commission[a] 2013, p. 3). Which they identify is mainly due to the borderless and multi-layered characteristics of the internet (European Commission[a] 2013, p. 3). Other than confirming the EU's strong believe in ICT's ability to spread ideas and values this also indicate why the EU is so interested in this aspect. The quote suggests that the EU interest comes from the fact that the spread of values will happen with a minimum of efforts and cost for the EU.

However, this is only possible if the internet stays open and free and this fact could be the explanation behind the Cybersecurity Strategy's strong support for the multi-stakeholder model is even stronger than in the DAE. Additionally, the EU makes it clear that the model is democratic as well as efficient in regards to governance (European Commission[a] 2013, p. 4). The fact that the EU view this internet governance model as democratic and wishes to promote it internationally indicates that the multi-stakeholder model is a part of the EU policy strategy to spread its values. To this, the EU explains that it will seek cooperation with international partners and here the EU presents the Council of Europe, UN, OSCE, OECD, AU, ASEAN and OAS[2] (European Commission[a] 2013, pp. 14-15). Firstly, this shows that the EU will not promote this by themselves, but maybe more interestingly they will push these organisations to support the idea. An interesting aspect of this presentation of international partners is the lack of institutions that is directly involved with Internet governance such as the Internet Corporation for Assigned Names and Numbers (ICANN) or the Internet Governance Forum (IGF). ICANN is maybe most interesting here because *"(...) it is a 'nonprofit public-benefit corporation'(...)"* (Klimburg and Tirmaa-Klarr 2011, p. 21) without government control[3]. IGF on the other hand (which the EU supported in the DAE) is a UN agency (Klimburg and Tirmaa-Klarr 2011, p. 21). The point here is that even though the EU supported the multi-stakeholder model and recognised that the governing of cyberspace is a shared responsibility it does not seem that the EU support is one hundred percent. Rather the EU support more traditional international institutions. However, the reason behind the EU's lack of backing to ICANN and similar institutions is elusive.

The section above should highlight that the EU has a stronger focus on the political/ideologic aspect of cyberspace in the Cybersecurity Strategy. Furthermore, these aspects follow the political/ideologic paradigm. To this, it is interesting to notice that regarding the Arab Spring the same event has shown totalitarian states that there is a need for stronger control over cyberspace. This aspect is however not discussed by the EU, but they do state that a more connected world should not be meet with increased censorship or mass surveillance (European Commission[a] 2013, p. 15). Another aspect the EU do

[2] Find full names in the glossary.
[3] The US government released ICANN in 2009 (Klimburg and Tirmaa-Klarr 2011, p. 21).

not address in the policy document is the fact that the same mechanism they want to exploited can be used by others e.g. terrorist. When the Cybersecurity Strategy was drafted the Islamic State (ISIS) was not a major international issue, however in recent times they have shown how effective they can use cyberspace to spread propaganda and recruit new people to their cause (Ashok, 2016, n.p). However, it was already acknowledged before 2010 that cyberspace could be used as a tool by terrorists (Reardon and Choucri 2012, pp. 22-24), yet the EU does not seem concerned about this possibility in its policy approach.

The Cybersecurity Strategy on Security Aspects

In regards to how the Cybersecurity Strategy presents security aspects is where some of the biggest developments are found. Firstly, the document presents both a definition of cybersecurity and cybercrime. These new definitions do not fundamentally change the EU's understanding of cyber security from the DAE. However, it clarifies it and supports the claim that security is more important in the Cybersecurity Strategy. It is acknowledged that cyber security naturally will play a role in a cybersecurity policy document, however, the fact that the EU has produced such a policy document is in itself a testimony of a changed perception of the need for security in cyberspace. Especially because the EU has limited influence in regards to national security and that its involvement in foreign policy is often perceived to be controversial (Christou 2016, p. ix-x; Sliwinski 2014, p. 471). The EU addresses this issue in the policy document by *"(...) acknowledging that it is predominantly the task of Member States to deal with security challenges in cyberspace, this strategy proposes specific actions that can enhance the EU's overall performance."* (European Commission[a] 2013, p. 4). The fact that the EU involve itself more despite of this, further supports the argument that the EU has gotten more concerned about the threats from cyberspace.

Albeit the EU recognises that they have a limited saying in cyber security they still involve themselves in national security issues in the Cybersecurity Strategy. This can be seen through the fact that one of the strategic points presented in the Cybersecurity Strategy is the creation of a common defence policy under CFDP as well as in the cyber security definition where it is stated. *"Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields (...)"* (European Commission[a] 2013, p. 3). Furthermore, the EU later explains *"(...) that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced."* (European Commission[a] 2013, p. 11). This shows that the EU recognised that both civilian and military involvement is needed to create a secure cyberspace.

This understanding was not present in the DAE and could suggest that one of the EU's policy aims is to involve itself in the military aspects of cyber security. Furthermore, by identifying the possibility of military threats could be an indication that the EU views cyberspace as a possible future battleground and thereby subscribes to the ideas of the security paradigm. However, the EU refrains from using words like cyber war, cyber warfare as well as framing a defensive approach towards building security (European Commission[a] 2013, p. 11). Not that the last aspect is excluded from the security paradigm, but it suggests that the EU does not want to be a part of a more militarised cyberspace.

To the observations above it is interesting to investigate how the EU envisions its involvement especially when this is such a sensitive area. First of all the EU argues that due to complexity and involvement of many actors on the issue "(…) *centralised, European supervision is not the answer*." (European Commission[a] 2013, p. 17). Instead, the EU want to be involved when a risk or threat has a cross-border dimension (European Commission[a] 2013, p. 5). This example could indicate that the EU's policy will have limited influence over the Member States. However, due to the borderless nature of cyberspace as well as the interdependence across member states one could argue that this approached is maybe not that limited. Which the EU later also confirms through the following quote: *"At the same time, due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement."* (European Commission[a] 2013, p. 17).

With the increased focus on security aspect in the policy document identifying what the EU perceives as risk and threats from cyberspace is relevant. There is a definition of cybercrime in the policy document as already mentioned and as with the cyber security definition, this could indicate that the EU is even more concerned about cybercrime than when the DAE was drafted. The definition however does not change what is perceived as threats from cyberspace in the DAE instead it specifies it. The definition highlight "(…) *traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)."* (European Commission[a] 2013, p. 3). To this understanding it is added that threats from cyberspace "(…) *can have different origins – including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes."* (European Commission[a] 2013, p. 3). This shows that EU's understanding of cybercrime, as well as its origins, has become more developed which again support the claim that the EU's policy is more focused on security and the threats from cyberspace. However, the fact that the EU chooses to define cyber crime and not any other threats from cyberspace suggest that its concern in regards to cyberspace is on criminal activities and how they affect the society and economy rather than a possible existential threat for the EU.

An argument behind the increased focus on security in the Cybersecurity Strategy is apparent in several examples. The EU e.g. states that "*Cybersecurity incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services.*" (European Commission[a] 2013, p. 3). What is new in this quote is that the EU starts to share some of the perceptions of cyberspace with the security paradigm and here more precisely the term 'cyber Pearl Harbor'. Cyber Pearl Harbor envision a devastating cyberattack that targets critical infrastructure with the aim of causing a total collapse of society (Loui and Loui 2016, p. 31). The EU never uses the term, but it is still indirectly present in the example by the reference to the disruption of these critical sectors. This indicates that the EU does not only perceive the threats from cyberspace as an economic threat but also as a security threat maybe even a possible existential threat. This negative perception is new, and it is a fairly big change from the optimistic view of the DAE. The example above is not the only example of this more negative perception in the policy document the EU e.g. also states that *"The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities (...)"* (European Commission[a] 2013, p. 4). This example further supports the observation and argumentation for a change in the EU's understanding of opportunities and threats in cyberspace.

Even though this more concerned and negative perception of the consequences is presented in the Cybersecurity Strategy, the EU still views cybercrime as the most present threat. It is stated that *"The more we live in a digital world, the more opportunities for cyber criminals to exploit. Cybercrime is one of the fastest growing forms of crime (...)"* (European Commission[a] 2013, p. 9) and that cybercrime is getting more sophisticated and the methods utilised by the criminals is evolving rapidly (European Commission[a] 2013, pp. 3, 9). This shows that cybercrime still is the primary threat identified by the EU which get further confirmed by the fact that the EU states that the European economy is already affected by it (European Commission[a] 2013, p. 3). Yet, this do not change that fact that in regards to security aspects one of the biggest policy changes can be seen from the DAE to the Cybersecurity Strategy and this change is maybe best shown in the following quote: *"Recent years* *have seen that while the digital world brings enormous benefits, it is also vulnerable."* (European Commission[a] 2013, p. 3).

Summary

As with the DAE, after presenting the paradigms found in the Cybersecurity Strategy, there is still a need for a discussion about the dominating paradigm. In the DAE the EU's perception of cyberspace was dominated by the social/economic paradigm. However, in the Cybersecurity Strategy arguments for the presence of all three paradigms has been found. Furthermore, it is not easy to determine which is the most dominant. The reason for this is that the focus on social/economic aspects is relatively limited in the policy document. On the other hand, both political/ideologic aspects and well as security aspects are highly present. But, it can argue that this is not a surprise due to the nature of the documents along with the involvement of the High Representative of the European Union for Foreign Affairs and Security Policy and the European External Action Service. Therefore, this observation does not give enough evidence to support one paradigm over the others.

However, there are arguments that support an exclusion of the security paradigm. Even though there was evidence of increased concern about the threat and risk coming from cyberspace along with the idea of serious cyber attacks against critical infrastructure, the general threat perceived by the EU comes from cybercrime. This fact does not follow the security paradigm, and it can therefore not be the most dominant. It is important to state that this does not undermine the observation that a change has happened in regards to how concerned the EU is about the risk and threats related to cyberspace.

There are however no good arguments for either the social/economic paradigm nor the political/ideologic paradigm to be dominant, and therefore no single paradigm will be picked. However, the strong presence of both paradigms indicates that the EU despite increased concern, still believe in the positive benefits and the ability to forward the EU's goal with the use of ICT's and cyberspace. This fact is maybe best shown in the last quotation from the security aspect section where the EU states that the digital world brings enormous benefits. Confirming that the EU is mostly focused on the positive benefits from cyberspace but acknowledges the threats.

3.3 Analysis of the Network and Information Security Directive

The same day (February 7, 2013) that the Commission published the Cybersecurity Strategy, they also released *a proposal for a Directive of the European Parliament and of the Council – concerning measures to ensure a high common level of network and information security across the Union.* It is this Directive – commonly known as the Network and Information Security Directive or simply NIS Directive – that this chapter will analyse. As with the previous chapters, this will start with a short presentation of the document followed by a brief review of the content. Then an analysis will be conducted on how the document presents EU's policy towards respectively social/economic aspects, political/ideologic aspects and security aspects along with how the findings follow the presented paradigms. Lastly, the observations from the analysis will be discussed to determine whether any paradigm is dominant in the NIS Directive.

NIS Directive Introduction

As with the other policy documents, this was also drafted by the European Commission. However, the NIS Directive is still very different due to it being a proposal for a directive. Directives are legislative acts that frames objectives which all the Member States are obligated to fulfil. Because it only frames the objective, each member state must form its laws to reach the goal of the directive (European Union[a] 2016, n.p.). The NIS Directive was negotiated through the ordinary legislative procedure meaning that the Council and the European Parliament must agree on the directive before it can be adopted (Wallace, Pollack and Young 2015, p. 73). The leading service behind the drafting of the proposal was Directorate-General for Communications Networks, Content and Technology. The proposal was sent to the European Parliament and the Council of the European Union and went through negotiations until 6. July 2016 where it was signed by the President of the European Parliament and the President of the Council.

The NIS Directive was published as a part of the actions taken by the Cybersecurity Strategy. This means that the objectives are closely related, but the aim of the document is more focused.

The NIS Directive's objective is to create a high level of Network and Information Security (NIS) across the European Union. This goal will be accomplished by obligating the Member States to establish (European Commission[b] 2013, pp. 2, 33):

- A competent national authority.

- A national CERT (Computer Emergency Response Team).
- A national NIS strategy.
- A national NIS cooperation plan.

Another part of the directive is to involve operators of critical infrastructure (energy, finance, health, and so forth) and providers of information services (search engine, social networks and so forth). These operators are obliged to report serious cyber incidents as well as to adopt proper steps to manage the security risks. (European Commission[b] 2013, pp. 2-4)

These aim of these objectives is to increase its preparedness and resilience of the Member States and due to the often cross-border nature of cyberspace, the overall resilience of the EU network systems will be increased. (European Commission[b] 2013, pp. 32-33)

With a basic understanding of the content and aim of the Directive, the analysis of the policy document can be conducted.

The NIS Directive on Social/Economic Aspects

The NIS Directive is presenting several arguments for the need for NIS in Europe. The arguments that the EU presents are mostly focused on social and economic consequences if the EU does not create enough NIS across the Member States. It is in this regard that the NIS Directive is linked to the DAE – by arguing for the need of action based on social/economic arguments. That this is a fact can be seen in this example:

"Network and information systems and services play a vital role in the society. Their reliability and security are essential to economic activities and social welfare, and in particular to the functioning of the internal market." (European Commission[b] 2013, p. 11).

This example confirms that the social/economic aspects are present in the policy document. Furthermore, this shows that the EU is concerned about the effects if network and information systems are interrupted. However, it is also clear that the EU is mostly concerned about the effect lack of NIS can have on the economy (internal market). This argument gets further supported by the following quote: *"This [Lack of NIS] can stop businesses functioning, generate substantial financial losses for the EU economy and negatively affect societal welfare."* (European Commission[b] 2013, p. 2).

This perception is somewhat comparable to the 'trust security' understanding present in the DAE. Meaning that NIS is needed to ensure the functioning of the economy, as trust and security were necessary to ensure the EU could harness the powers of ICT's. The point here is that security is a means to an end and in this regard to secure the economy. Which thereby indicate that the EU's policy follows the social/economic paradigm. This observation gets further backed by the fact that the EU states that "*The likelihood and frequency of incidents and the inability to ensure efficient protection also undermine public trust and confidence in network and information services.*" (European Commission[b] 2013, p. 3). This argument by the EU is followed by results from a survey confirming that the European citizens are concerned about security in regards to online payment along with buying stuff online or using online banking due to the security risks (European Commission[b] 2013, p. 3). Hereby confirming the observation and argumentation above.

With the social/economic paradigm, strongly present in both the DAE and the NIS Directive and to a more limited extend in the Cybersecurity Strategy it could be concluded that the EU, in general, is mostly focused on the social/economic aspects and how the emergence of cyberspace has and can affect the functioning of these areas. However, the NIS Directive presents another explanation for this strong focus – legitimacy. As discussed in the Cybersecurity Strategy one of the issues faced by the EU in regards to cyber security is the limited influence it has on national security as well as national defence policy of the Member States. Hence, the EU frames this as an economic issue, to gain more legitimacy to act on the area. This is possible due to Article 26 and Article 114 under the Treaty on the Functioning of the European Union (TFEU) which the EU also refers to in the NIS Directive (European Commission [b] 2013, p. 8). With these Articles the EU explains that they are empowered *"(...) to adopt measures with the aim of establishing or ensuring the functioning of the Internal Market (...)*" (European Commission [b] 2013, p. 8). The point here is that the renewed focus on the social and economic consequences which was not as present in the Cybersecurity Strategy can be explained by a need to create legitimacy. However, this does not change the fact that the policy in the NIS Directive follows the social/economic paradigm.

Even though that some of the observation above show that there are similarities between the DAE and the NIS Directive the more negative view on cyberspace from the Cybersecurity Strategy is also present in the examples above. It could be argued that this is simply due to the nature of the policy document being focused on NIS. However, it must be remembered that the NIS Directive along with the Cybersecurity Strategy are a representation of the EU's perception of the time or in other words that they saw a need for a directive forcing the Member States to create more security.

The NIS Directive on Political/Ideologic Aspects

One aspect that has gotten attention in the previous policy documents is the political/ideologic aspect, however, in the NIS Directive, it does not get the same attention. The simple explanation is that due to the nature of the document it is more internally focused rather than externally. It must be stated that this does not suggest that the EU cannot follow the political/ideologic paradigm which e.g. acknowledges that the spread of values can be a threat. However, even with the internal focus the NIS Directive also has an international dimension to it which can be seen in this quote:

"(...) by putting its own house in order, the EU would be able to extend its international reach and become an even more credible partner for cooperation at bilateral and multilateral level. The EU would hence also be better placed to promote fundamental rights and EU core values abroad." (European Commission[b] 2013, p. 8).

This again confirms the idea that the EU wants to use cyberspace as a tool to spread its values and it thereby also shows that the EU still follow some of the lines of the political/ideologic paradigm in the NIS Directive. Furthermore, the EU later explains that the EU's aim is to promote NIS internationally with the hope of creating a higher common level internationally (European Commission[b] 2013, p. 14). This shows that the EU's international policy is not only focused around the wish to spread values but also to build security. Additionally, in the NIS Directive, it is worth noting that the EU approached is based on the multi-stakeholder model, which is apparent in the fact that the EU involves non-governmental actors in the strategy (see content presentation). Therefore, it can be argued that the EU's policy on promoting NIS internationally will also support the EU policy on promoting its values.

The section above should show that political/ideologic paradigm is still present in the NIS Directive even though the policy document has a limited focus on the aspects. However, it is interesting to note that the NIS Directive does not mention that the internet should be kept open and free. For some reason, the NIS Directive has left this out which is peculiar when it is taken into consideration the focus it had in the other documents – especially the Cybersecurity Strategy where it was in the title. It can be argued that the aim of the Directive which is to create more secure network and information systems does not fit with the idea of an open and free internet. This suggests that the EU acknowledges this fact and therefore leave it out. However, it is still present indirectly through the support of the multi-stakeholder model as well its continued goal of promoting fundamental rights and its values through cyberspace. The point is that the EU knows that its policy approach has some contradiction in regards to its aim of building security and securing the open and free characteristics of cyberspace.

The NIS Directive on Security Aspects

Even tough the NIS Directive is closely linked to the Cybersecurity Strategy it still presents some new perspectives on the EU's policy towards cyberspace. The EU does for example not refer to cyber attacks in the policy documents rather the stick to cyber incidents which they describe as *"(…) any circumstance or event having an actual adverse effect on security;"* (European Commission[b] 2013, p. 19). The EU has properly chosen 'incidence' rather than cyber attack due to the policy document being a legislative act, which therefore creates a need for clarity. The EU states that *"(…) information systems can be affected by security incidents, such as human mistakes, natural events, technical failures or malicious attacks."* (European Commission[b] 2013, p. 2). This example shows the issues with the use of cyber attacks because security risk and threat can also be accidental or technical. This understanding suggests that the EU does not follow the security paradigm in the NIS Directive. To further support this claim, the EU again show that its major concern is still cybercrime by stating that *"Criminal activities are in many cases underlying an incident."* (European Commission[b] 2013, p. 15). To this the EU adds that cyber incidents are increasing in size, rate and complexity (European Commission[b] 2013, p. 2). This confirms that the EU is concerned about the effects that cyber incidence has but also can have in the future. Thereby supporting a change of perception already found in the Cybersecurity Strategy. However, it must be stated that in the NIS Directive the EU never highlights the possibility of more severe consequences than financial loss or loss of societal welfare. Hence there is no evidence to support that the EU's policy follows the lines of the security paradigm.

The fact that incidence is becoming more frequent is also one of the major arguments behind the EU's claim behind the need for more resilient systems in the EU. The resilience approach is based on the idea of creating a system that can bounce back and recover after an incidence (Dunn Cavelty 2013, pp. 5-6). This definition shows that resilience is a defensive approach. Furthermore, it can be argued that that the EU follows it because it will help them in securing that social and economic systems do not get interrupted. Thereby reinforcing the argument of the focus on social/economic aspects in the NIS Directive.

In relation to the observation about the EU refraining from using the term cyber attack, it is interesting to notice that the EU does not use 'threat' either. This is interesting because this is the first time the EU does not use threats - which they have not been reluctant to use before. One reason behind this could be due to the slightly different meaning of risk and threat. According to Mikkel Vedby Rasmussen (2001) the use of threat and risk highlights how imminent the danger is. A threat is understood as direct and impending where risk is more distant and accidental (p. 293). The lack of the word 'threat' could indicate an attempt to not inflate the issue in relations to the consequences of a cyber incidence. This shows that the EU at least to some extend tries not to exaggerate the security risks related to cyberspace. That this is a fact gets further supported by the previous observation that the EU does not use the term cyber attack either. Furthermore, this could suggest that the EU is still more interested in the positive aspects and opportunities from cyberspace rather than concerned about the threats.

The evidence found in this section does not support that the EU's policy presented in the NIS Directive follows the security paradigm. Instead the findings above only further support the claim of a strong presence of the social/economic paradigm.

Summary

Now that an understanding of the EU's policy approach in the NIS Directive has been given along with an analysis of which paradigms are present in the document a short discussion of the dominating paradigm has to be conducted.

The first observation is that the NIS Directive is placing itself in the middle of the DAE and the Cybersecurity Strategy. It has a strong focus on social and economic aspects and mainly follows the ideas social/economic paradigm which were also observed in the DAE. The findings also showed that the political/ideologic paradigm along with a focus on security and adverse consequences of a cyber incidence - from the Cybersecurity Strategy - was present in the NIS Directive. In this perspective, the NIS Directive is in some way forming a bridge between the two prior policy documents.

However, it is argued that the dominating paradigm in this policy document is social/economic. The reason for this is due to the aim of the NIS Directive which is to create NIS because it *"(…) can stop businesses functioning, generate substantial financial losses for the EU economy and negatively affect societal welfare."* (European Commission[b] 2013, 2). This is the best evidence for claiming that the social/economic paradigm is the dominating paradigm in the NIS Directive. However, the fact that the political/ideologic aspect is present in the document is a testimony in itself to how important the EU view this aspect of its policy.

The NIS Directive does not present any major change to the EU policy approach and perception of cyberspace. However, it confirms the findings of the previous analysis and gives additional evidence to the conclusions and here most importantly that the EU's policy follows the lines of the social/economic paradigm. Furthermore, it shows that the EU even though more concerned is still focused on harnessing the opportunities connected to cyberspace and minimise the threats.

4.0 Discussion

The following section will discuss the findings of the analysis of the EU's and answer the problem formulation of this project. To answer the question, the central observation from each analysis of the policy documents will be discussed and put into relation to each other to determine any change in the EU's policy approach. Furthermore, it will be discussed which paradigm, if any, that is dominating throughout the documents and what that tell about the EU's policy.

In the analysis of the DAE, it was argued that the EU had a strong focus on the social/economic aspects and that the EU's policy approach, in general, followed the social/economic paradigm. The political/ideologic paradigm was also present in the DAE however, the findings from the two other policy documents showed that the EU got a stronger focus on this aspect after 2010. However, the presence of both paradigm along with how the EU presented its policy in the DAE suggest that the EU saw cyberspace as a tool or opportunity to solve several issues that they faced at the time. This fact is further supported by the observation from the section that investigates how the EU understood the security aspects of cyberspace. The findings show that security was understood as a means to an end – getting the European citizens to use ICT's. There are no indications for any major security concerns in the DAE. However, this does not mean that the EU does not acknowledge that there are risks and threats in relation to cyberspace.

Yet, the question still stands why the EU so strongly follows the social/economic paradigm in the DAE. It can be argued that the threats from cyberspace along with the serious effects of a cyber attack should be apparent to the EU, in particular, due to the cyber attack in Estonia and Georgia. So why is the EU more focused on the opportunities rather than the threats?

A possible explanation is that the EU wants to use cyberspace to resolve the problems related to the EU crisis. This is no surprise since the EU clearly states this in the DAE, but what is interesting is that the Eurozone crisis was more than just an economic crisis. The crisis also highlighted other issues and in particular the democratic deficit in the EU (Bellamy n.d., p. 3; Cramme and Hobolt 2014, p. 1). Due to this fact, it is interesting that the social/economic paradigm, as well as the political/ideologic paradigm, is present in the DAE. It suggests that the EU perceives cyberspace as a communication- and trading tool and furthermore see these characteristics as a way to solve financial, societal and political issues that emerged with the Eurozone crisis. This fact could also explain why the EU were not that concerned about the threats and risk related to cyberspace because its focus was on other issues that needed to be solved at that time. This indicates that the EU followed the optimistic view of the possibilities related to cyberspace and ICT's which is often present in the social/economic paradigm. This fact implies that the EU hoped that cyberspace and ICTs could help to solve the problems it faced at that time. Meaning that the EU's policy approach was formed by this perception that highlights possibilities of cyberspace rather than threats.

The argumentation for the EU's perception and policy approach towards cyberspace observed in the DAE could also be a part of the explanation for the located changes in the Cybersecurity Strategy. However, before this is discussed, it must be stated that even though a change in the EU's perception of cyberspace was observed it did not change which paradigm the policy followed. What the analysis found was that all three paradigm was present in the Cybersecurity Strategy, but it was argued that it was the social/economic- and political/ideologic paradigm that was most dominant in the EU's policy approach. The changes were regarding the security aspect and the EU's view on risk and threats from cyberspace. The findings indicated that the EU has become more concerned about the threats from cyberspace which the document in itself is a testimony too. Furthermore, with the Eurozone crisis more in the background and the fact that the EU in 2011 experienced several attacks against its institutions along with a cyber attack where emission allowances worth €30 million was stolen from the EU's emissions trading scheme (Christou 2016, p. 2) could be the reason behind the change in EU's perception of cyberspace and thereby also explain the change in its policy approach to focus more on creating security. The argument here is that constructivism believes that when an actor's perception change towards an object so will its action (Wendt 1992, p. pp. 396-397). Additionally, it is worth adding that Christou's book states that the attacks *"(...) on its own institutions in 2011, among other high-profile cases, provided a wake-up call for the EU (...)"* (Christou 2016, p. xi) and this lead to an increased focus on cyber security in the EU's. This further supports the results from the discussion above.

The same argument in regards to constructivism can also help to explain why the Cybersecurity Strategy has an increased focus on promoting democratic values internationally. The Arab Spring (which the EU itself refers to as an example) has shown that cyberspace can promote and forward democratic values and thereby confirmed the EU that cyberspace had this capacity. By once again applying Wendt's fundamental principle of constructivism (as it was done above) the change in EU's perception can be credited to an event which in this regard was the Arab Spring. This change of perception lead, maybe not to a different policy approach, but a stronger focus on promoting an EU foreign policy that promotes cyberspace as open and free.

The results from the analysis of the NIS Directive did not present any change to the findings from the two previous analysis. However, it can be argued that the analysis of the NIS Directive confirm the observations from the other analyses. The social/economic paradigm was still present along with the political/ideologic paradigm. In regards to the security aspects, the same perception from the Cybersecurity Strategy was present, but there were no indications that the policy approach followed the security paradigm.

To collect the results from the section above. The EU's policy approach has changed as well as the EU's perception of cyberspace to one more focused on security. However, the fact that the EU throughout its policy documents follows the social/economic paradigm along with the political/ideologic suggest that the overall goal that the EU wants to achieve has not changed. The EU wants to harness the opportunities which has developed with cyberspace and ICTs while minimising the threats.

The section above has again highlighted the significant findings from the analysis and further discussed why the EU's perception and policy have changed in the period. However, why does the EU follow the lines of the social/economic- and political/ideologic paradigm in the policy documents especially when it is known the EU's perception is contested by many nations – at least in regards to the open and free internet? It is here that the theory of constructivism can help to further explain the EU's choices. Eriksson and Giacomello explains that constructivism do not have *"(...) a core (...) theorem on what forces shape world politics (...)"* (Eriksson and Giacomello 2010, p. 18), but if one should be given it would follow this logic: Actors has ideas of what is right and wrong based on a set of norms. These norms shape an identity by creating an 'us' and a 'them'. Lastly, the identity forms the actor's interest. Being socially constructed these aspects must be understood as dynamic, meaning that if the interests of an actor change it is because of a change in its norms and identity (Eriksson and Giacomello 2010, p. 18). So, which norms guide the EU identity? The EU states that it was stated as an economic union but later has developed to a political one and is now involved in areas such as economic, environment, health, foreign policy and security and promotes human rights and equality internally and externally (European Union[b] 2016, n.p.). Which means that the EU identifies itself as an economic and political union. Then if the constructivism 'theorem' is applied to the findings of this project shows that the EU's identify guides its interest. This explains the EU's focus on the social/economic- and political/ideologic paradigm it is a part of its identity. This shows that constructivism can help explain actors action in regards to cyberspace.

Thereby it has been shown that constructivism can help to explain why the EU stuck to the social/economic paradigm along with the political/ideologic paradigm which was as a consequence of its identity as a liberal democracy. However, the change from an optimistic policy approach to a policy more focused on security is due to certain events that altered the EU risk and threat assessment in regards to cyberspace.

With all aspects of the analysis discussed it is now possible to collect the findings and answer the problem formulation of this thesis. This will be done in the next chapter.

5.0 Conclusion

This section will collect the findings from the project to answer the problem formulation: *How does the European Union present its policy towards cyberspace in their policy documents in the period 2010-2013 and has the policy changed? Additionally, how does the European Union's policy follow some of the general paradigms of understanding cyberspace and what does that tell about the European Union's perception of the emergence of cyberspace?*

In regards to understanding cyberspace, three paradigms were located: social/economic-, political/ideologic- and security paradigm. Each of these paradigms represents different ways of understanding the effect of cyberspace. In this project, paradigm was not used as restrictively as it was constructed by Kuhn meaning that even though a community of people followed the social/economic paradigm did not mean that they did not recognise the other effects of cyberspace. The paradigms were constructed with the aim of getting a deeper understanding of the EU's perception along with its policy towards cyberspace by putting the findings into perspective.

The discussion found that the EU's perception and policy approach towards cyberspace had changed in the period. In the DAE the EU had an optimistic understanding with little concern about the threats from cyberspace. This changed in the Cybersecurity Strategy and NIS Directive to a policy more focused on minimising risk and threats from cyberspace. That EU's policy approach has changed is maybe best shown by the fact that the EU created a cyber security policy along with a directive which changed the EU's approach from a voluntary to an obligatory. This suggests that the EU has become more concerned and more focused on combating the risk and threats emerging from cyberspace. However, it was still argued that since all the analysed policy documents followed the social/economic paradigm along with the political ideologic the goal of EU's policy is still to harness and exploit the opportunities of cyberspace and ICT's.

So, to the answer, this project problem formulation: The EU's policy approach towards cyberspace in the period 2010-2013 has changed. The change was from a positive perception of cyberspace focused on exploding ICT's and cyberspace in the DAE to one more focused on security and limiting the threats and risks from the domain in the Cybersecurity Strategy and NIS Directive. Nevertheless, it was found that the EU followed the ideas of the social/economic and political/ideologic paradigm. This fact indicates that the EU's goal still is to profit from the opportunities inherited in cyberspace.

The aim of this project was to show how the EU has reacted towards the emergence of cyberspace by analysing how they had written about the domain in its policy documents in the selected period. Because this method was used the IR theory of social constructivism has been the theoretical background for this project. This project has shown the relevance that the theory can play in not only investigating and explaining an actors approach towards cyberspace but has given a deeper understanding of how cyberspace is understood through the three identified paradigm. Therefore, this project can furthermore confirm the relevance of using constructivism in explaining the emergence of cyberspace as Eriksson and Giacomello also perceived it.

Limitation

This project has investigated the EU's policy approach towards cyberspace. However, it must be said that this project has not taken into consideration how particular institutions in the EU view cyberspace or whether the Member States shares the view of the EU. Hence the findings are limited to the general perception shared by the EU as an institution and as presented through its policy documents.

Furthermore, the policy documents used in this project has been the major policy documents which directly addresses the subject area. However, the EU has in the period create other documents which directly or indirectly has addressed areas concerning cyberspace. The point is that other policy documents can be located and the findings in this project have not taken all the EU policy documents into consideration. The point is that the EU can have addressed other areas than presented in this project. However, it is believed that the selected policy documents show how the EU envisions its general policy approach towards the area hence the findings are still valid and highly relevant.

6.0 Perspectivation

This project has shown that the EU perception of cyberspace is developing and it was found that this change could be attributed events happening internally or externally. However, the findings of this project represent the EU's policy and understanding of cyberspace in the given period meaning that it can have change. Especially with the knowledge that these policy documents were produced before the Snowden Revelations in 2013 (Dunn Cavelty, p. 3). Due to the nature of this incidence, it could be imagined that now and in the future, the EU is even more obligated to its continued support for the open and free nature of cyberspace along with policies fighting mass surveillance. However, as stated in this project the EU's approach is contested, and this has only gotten worse as governments scramble to gain more security in and from cyberspace. Even though the EU's perceptions are challenged, it is difficult to image that the EU will change its policy and support claims for more government control. The point here is that this goes against the EU's values, norms and ideas and would severely challenge the EU's identity. Due to this fact, it is argued that the EU's perception of cyberspace can have changed since 2013, but it would still follow the lines of the findings of this project.

Future research

One of the goals of this project was to address some of the basics due to the limited amount of research available especially in regards to the EU and how it has handled the emergence of cyberspace. Due to this goal, it has also been found highly relevant to present some possibilities for future research.

The paradigms helped to get a deeper understanding of the EU's policy approach towards cyberspace. However, another interesting approach could be a comparison with other international actors. This could, for example, be some of the big cyber actors such as the US, China, Russia. However, it is acknowledged that this could have some complications due to EU's intergovernmental characteristics. Due to this fact, the EU could be compared to other international institutions such as NATO or UN. The approaches above could help to highlight how other nations or institutions perceive the emergence of cyberspace and how they envision that cyberspace should be governed compared to the EU. This again could help to understand how cyberspace will develop in the future because how the actors perceive it will determine its actions towards it and cyberspace can be changed (Deibert 2013, p. 529).

Furthermore, in regards to European Studies an analysis of the cyberspace policies of the Member States could be interesting. Such an approach would not only tell something about how the Member

States perceive cyberspace but if compared with the findings of this project it would also show how well the EU can transfer its ideas and values inside the Union.

Other approaches could be more meta-oriented. Firstly, a project focusing like Reardon and Choucri's on themes in the research literature could be highly relevant with the increase of literature released the last couple of years. The research could either have a focus on research on the EU and cyberspace or simply on recent cyber IR literature. Such project is highly valuable due to the that the field is still underdeveloped and such a project can thereby guide scholars into areas that need further research.

There is also a need for research focusing on the development of a better method of analysing cyberspace along with how IR theories can be applied. Additionally, this project has also opened up for the idea that different paradigms exist in regards to understanding the consequences and effect of cyberspace. It is acknowledged that further research is needed and that this aspect could have been a project by itself. Therefore, it is supported that a project based on this idea is constructed. It is believed that such a project could help to get a thorough understanding of cyberspace as well as the actions taken by different cyber actors.

Cyberspace is new, and it is still evolving. Hence there is still a vast amount of under answered question that needs to be addressed and the section above only scratches the surface. The current project is a starting point in the assessment of these questions.

7.0 Bibliography

Ashok, I., (2016), The anatomy of a 'Cyber Jihad' – analysing the evolution and future of terroism in cyberspace, in, *International Business Times*, 20-06-2016. Avalaible at: http://www.ibtimes.co.uk/anatomy-cyber-jihad-analysing-evolution-future-terrorism-cyberspace-1566184 (Accessed 13. December 2016)

Bellamy, R., (n.d), The Democratic Deficit, Social Justice and the Eurozone Crisis, in, *The Eurozone Crisis and the Democratic Deficit*, eds, Bellamy, R., and Staiger, U., London's Global University.

Bryant, C. G. A., (1975), Kuhn, Paradigms, and Sociology, in, *The British Journal of Sociology*, Vol. 26, No. 3, (September 1975), pp. 354-359.

Choucri, N. and Clark, D. D., (2012) Integrating Cyberspace and International Relations – The Co-evolution Dilemma, in, *Explorations in Cyber International Relations*, Massachusetts Institute of Technology, (November 2012).

Christou, G., Croft, S., Ceccorulli, M. and Lucarelli, S., (2010), European Union Security governance: putting the 'security' back in, in, *European Security*, 19:3, pp. 341-359.

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

Cramme, O. and Hobolt, S. B., (2014), *A European Union under Stress, in Democratic Politics in a European Union Under Stress*, eds. Cramme, O. and Hobolt, S. B., Oxford.

Deibert, R. J., (2003), Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace, In, *Millennium – Journal of International Studies*, Vol. 32, No. 3, (December 2003), pp. 501-530.

Demchak, C. C. & Dombrowski, P., (2011), Rise of a Cybered Westphalian Age, In, *Strategic Studies Quarterly*, (Spring 2011).

Dunn Cavelty, M., (2013), A Resilient Europe for an Open, Safe and Secure Cyberspace, in, *Occasional UI papers*, The Swedish Institute of International Affairs, vol. 23, (December 2013).

Eriksson, J. and Giacomello, G., (2010), Introduction: Closing the gap between international relations theory and studies of digital-age security, in, *International Relations and Security in the Digital Age*, eds. Eriksson, J. and Giacomello, G., Routledge.

European Commission, (2010), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*, Brussels, COM(2010)245 final.

European Commission[a], (2013), *Joint Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions – Cybersecurity*

Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, JOIN(2013) FINAL.

European Commission[b], (2013), *Proposal for a Directive of the European Parliament and of the Council - concerning measures to ensure a high common level of network and information security across the Union*, Brussels, COM (2013) 48 final.

European Commission[a], (2016), *Internet of Things*, n.d. Available at: https://ec.europa.eu/digital-single-market/en/internet-things [Accessed 27. November 2016].

European Commission[b], (2016), *Europe 2020*, 16-09-2016, Available at: http://ec.europa.eu/europe2020/index_en.htm, [Accessed 13. October 2016].

European Judicial Network, (2016), *Glossary*, n.d., Available at: http://ec.europa.eu/civiljustice/glossary/glossary_en.htm#Communication, [Accessed 14. October 2016].

European Union[a], (2016) *Regulations, Directives and other acts*, 22-11-2016, Available at: https://europa.eu/european-union/law/legal-acts_en [Accessed 22. November 2016]

European Union[b], (2016), *The EU in brief*, 15-12-2016, Available at: https://europa.eu/european-union/about-eu/eu-in-brief_en [Accessed 15. December 2016].

Eun, Y. & Aβmann, J. S., (2015) Taking Stock of Security and Warfare in the Digital Age, in, *International Studies Perspectives*, pp. 1-18.

Gibson, W., (1984) *Neuromancer,* HaperCollins Publishers.

Internet Live Stats, (2016), Live, Available at: http://www.internetlivestats.com/ [Accessed 28. September 2016].

Klimburg, A. and Tirmaa-Klarr, H., (2011), *Cyber Security and Cyberpower Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, DG for External Policies, Policy Department, European Union, (April 2011).

Klimburg, A., (2013), *Internet Yalta*, Center for a New American Security, (February 2013).

Kremer, J. F. & Müller B., (2014), *Cyberspace and International Relations,* Springer.

Kuehl, D. T., (2009), From Cyberspace to cyberpower: Defining the Problem, in, *Cyberpower and National Security,* eds. Kramer F. D. , Starr, S. and Wentz, L. K., National Defense UP.

Kuhn, T. S, (1970), *The Structure of Scientific Revolutions*, Second Edition, Vol. 2, No. 2, International Encyclopedia of Unified Science.

Lewis, J. A., (2014) Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms, Center for Strategic & International Studies.

Lotrionte, C. and Maurer, T., (2012), Building Trust in Cyberspace, in, *Georgetown Journal of International Affairs, International Engagement on cyber 2012: Establishing Norms and Improving Security*, George Town University Press, pp. 1-4.

Loui, R. P. and Loui, T. D., (2016), How to Survire a Cyber Pearl Harbor, in, *Computer*, Vol. 49, issue 6, (June 2016).

Maass, P. & Rajagopalan M., (2012), *Does Cybercrime Really Cost $1 Trillion?*, ProPublica, (August 2012), available at: https://www.propublica.org/article/does-cybercrime-really-cost-1-trillion

McAfee, (2013), *The Economic Impact of Cybercrime and Cyberespionage*, Center for Strategic and International Studies, (July 2013), available at: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

Morgan, S., (2016), *Cyber Crime Costs Projected to Reach $2 Trillion by 2019*, Forbes, (January 2016), available at: http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#12e0c1083bb0

Nye, J. S., (2010) *Cyberpower*, Belfer Center for Science and International Affairs.

Rasmussen, M. V., (2001), Reflexive Security: NATO and International Risk Society, in *Journal of International Studies*, Vol 20, No. 2, p. 285-309.

Reardon, R. & Choucri, N., (2012), *The Role of Cyberspace in International Relations: A View of the Literature*, Department of Political Science, MIT.

Sliwinski, K. F., (2014), Moving beyond the European Union's Weakness as a Cyber-Security Agent, In, *Contemporary Security Policy*, Vol. 35, No. 3, Taylor & Francis, pp. 468-486.

The White House, (2009), *The Comprehensive National Cybersecurity Initiative*. Available at: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Wallace, H., Pollack, M. A. & Young, A. R., (2015), *Policy-Making in the European Union*, Seventh Edition, Oxford University Press.

Wendt, A., (1992), Anarchy is what States make of it: The Social Construction of Power Politics, in *International Organization*, Vol. 46, No. 2, (Spring 1992), The MIT Press, pp. 391-425.