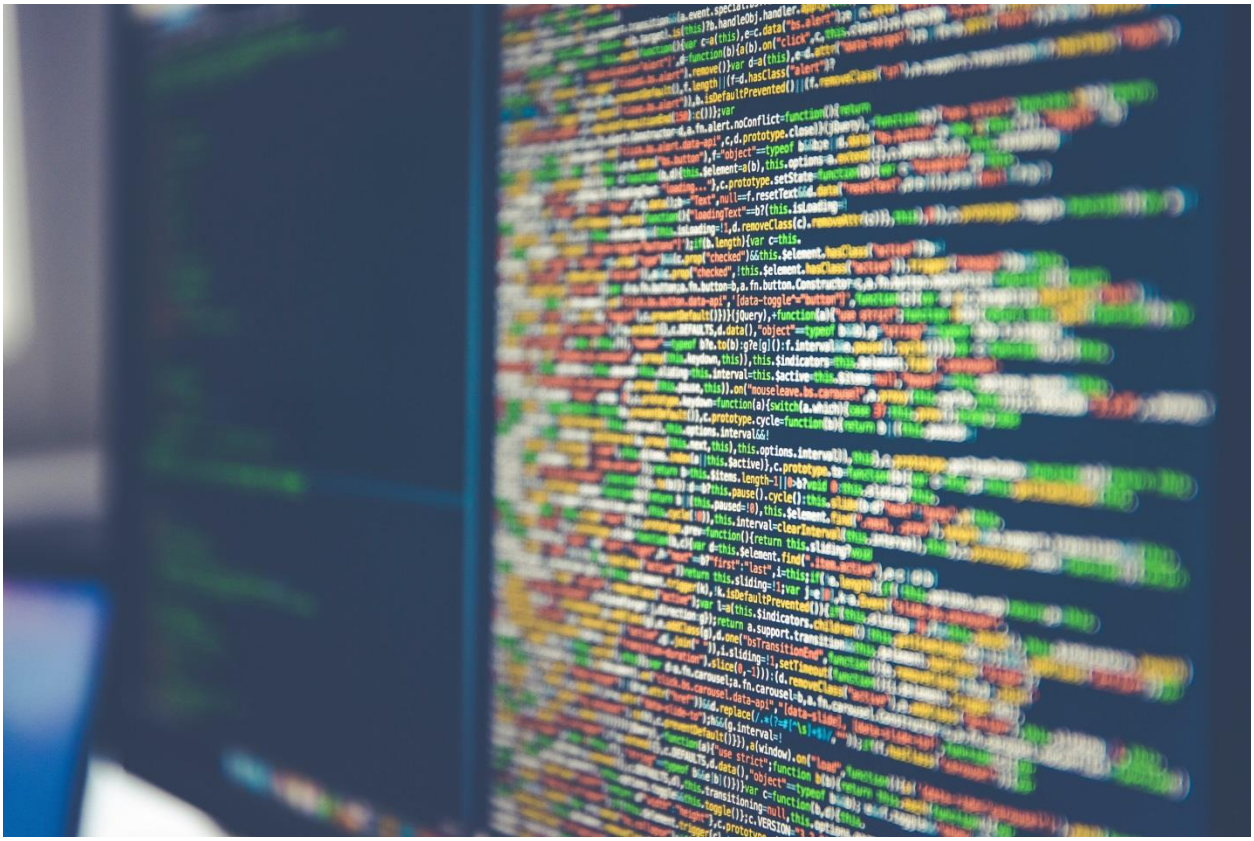

Cooperation in European Cyber Security: An International Relations Perspective on Collective Cyber Security in the European Union.

Kristian Linnet Eltzholtz

MA Thesis

Master's Programme in Culture, Communication and Globalization

Supervisor: Osman Farah

Spring 2017

Abstract

The topic of this thesis is collective cyber security under the framework of the European Cyber Security Strategy. The purpose of this study has been to analyse the obstacles to cooperation between the selected Member States and the strategy in question, specifically in regards to the challenges this presents the institutional attempt to establish a collective framework of cyber security in the European Union. These obstacles have been noted in the related literature.

In respect to this problematisation, the thesis has employed a comparative case study analysis, where the official documents of the respective strategies have been analysed, with a focus on specific provisions that reference cooperative engagement in European cyber security. The main focus of this approach has been to assess the intent of these strategies, and thus engagement with the European strategy. As an extension of this, the provisions detailing international cooperation, national interests, national security, and sovereignty have been taken into account for the individual national cyber security strategies, in order to assess the implication of these provisions for cooperation in the wider European strategy. These provisions, informed by the theoretical perspectives can then be grouped into dimensions of cooperation and conflict, with the purpose of an assessment of how the national strategies engage with the European strategy.

The thesis has used a pragmatic international relations theory epistemological approach, with the purpose of analysing the mentioned strategies from the theoretical positions of liberalism and realism. The theory of cyber power has been included to add an additional perspective on the use of soft power in cyber security, and to engage with the cyber security

literature. Following the application and engagement with theory, sub-conclusions based on the literature, theory, and analysed cases have been linked in a final conclusion on the findings.

In these findings, it has been established that the European strategy employs a liberal institutionalist framework. However, conflicting approaches to cyber security can be observed in the individual national strategies. While the selected cases refer to supranational cyber security engagement, each strategy presents its own obstacles to cooperation. In the UK strategy this is presented through its own guiding principles on cyber security in the London Conference, as well as an informal approach to cooperation with the European strategy. The findings from the German strategy point to an external policy, focusing on domestic interests in the international sphere. This is coupled with an ambition to maintain offensive cyber capabilities as a form of national interest in cyber security and wish to maintain sovereignty. The case of the French strategy also highlights a state-centric approach, while seemingly merging this approach with a liberal institutionalist framework for engaging with its private sector in cyber security areas of interest. In this, sovereign information is regarded as a particular national interest. Cyber security is also regarded as a priority in line with nuclear deterrence, as evidenced by the French white paper, laying the foundation for the strategy. The strategy also refers to international cyber security engagement through French values.

Based on these findings, coupled with the theoretical perspective, areas of Member State cooperation with the European strategy have been identified in provisions that follow the liberal institutionalist underpinnings of this strategy. These are demonstrated in the form of information sharing, acknowledgement of a need to situate the strategies in an institutional framework, as well as engagement with non-state actors in the form of organisations and civil society. Areas of conflict have been noted as national interests, driving parts of the international engagement in these cyber security strategies. This includes uses of cyber power to further these interests in institutions, as well as setting guiding principles for cooperation in this domain.

Finally, it has been pointed out that the observations made in the analysis are contextual to the topic of cyber security, specifically in regards to the established literature on this topic. This has also presented challenges for the application of international relations theory, as the internet as a permeating technology presents unique challenges to states and institutions. This has also been observed in the selected cases, where these strategies base principles of cyber security on liberal institutionalism, and specifically complex interdependence through transnational

cooperation with state and non-state actors. It has been demonstrated that these states seek to protect their national interests and sovereignty as concepts redefined in cyberspace, either through concerns of privacy in relation to citizens or cyber/military capabilities. In this case, it could be useful to provide other avenues of research such as securitisation theories and constructivism to also explore the social processes in CS

Table of Contents

Introduction

Cyber security (CS) has become a pressing issue as an increasing amount of information technologies have become embedded in the societal and economic aspects of Europe, according to the Cyber Security Strategy of the European Union.[1] Not only is this seen in how multiple European Member States (MS) have developed internal and external cyber policies that seek to regulate and establish a degree of control in cyberspace[2], but it is also seen with the involvement of their societies and how critical infrastructures in society have become connected to cyberspace, sometimes leading to vulnerability to disruption through cyber-attacks, such as the Stuxnet hacking attack which led to the temporary breakdown of the Natanz nuclear power plant in Iran.[3] Since then, national CS strategies have referenced these large-scale cyber-attacks to reinforce the argument for protective measures against threats in cyberspace. This can be observed in both the French[4] and German[5] strategies.

The rapid evolution of technology and possibilities for societies engaging with cyberspace has thus led to states adopting CS frameworks. However, as the nature of internet is transboundary and can be accessed from almost any location in the world, it has then led to several cooperation initiatives throughout the world which has resulted in both treaties and multilateral arrangements that seek to address the issues that are attached to cyberspace. This

[1] Appendix 1, p 2
[2] Ibid, p 3
[3] Karsten Friis and Jens Ringsmose, *Conflict in Cyber Space: Theoretical, strategic and legal perspectives* (London: Routledge, Taylor & Francis Group, 2016), p 2
[4] "France Cyber Security Strategy," France Cyber Security Strategy - ENISA, October 19, 2015, accessed March 15, 2017, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf/view, p 7
[5] "Cyber Security Strategy for Germany," Cyber Security Strategy for Germany - ENISA, February 20, 2014, accessed March 12, 2017. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-strategy-for-germany/view, p 2

thesis will look at CS cooperation in the European Union, specifically through the framework of the European Union Cyber Security Strategy of 2013 (EUCSS).

This strategy serves as the overall framework of European CS, together with the Directive on Security of Network and Information Systems (NIS-Directive).[6]

The European strategy seeks to increase CS in the EU through the exchange of information, cooperation, preparedness, and increased capabilities in cyberspace. This is further strengthened by increased cooperation between the public and private sectors in EU MS, thus aiding the security of the Digital Single Market.[7] Finally, the EU seeks to promote its core values and define norms for responsible behaviour, as well as advocate for the already existing international law in cyberspace, and help non-EU nations build their CS capacity.[8] The NIS-Directive adopted by the Parliament July 6, 2016 then provides the legal tools to enforce CS rules across the EU. MS are given 21 months to apply the Directive to their national laws and an additional 6 months to identity operators of their essential services.[9] The idea is to enforce CS cooperation through the establishment of Computer Security Incident Response Teams (CSIRT) and CSIRT networks for communication between these teams, and cooperation groups to exchange information.[10]

The aim of the thesis is to find out how CS in the EU is used as a space for both cooperation and contestation between EU MS. In relation to this, scholars have highlighted cooperation and coordination challenges of the EUCSS. One major factor in these challenges has been the cases of certain EU MS such as Germany, France, the U.K (as part of the internal market) that have established their own CS national plans, where certain provisions contradict the EUCSS. This takes place through their emphasis on national interests in CS.[11] These cases have also been noted as "double-paths" in the literature, which describes how these EU MS

[6] "Cybersecurity," Digital Single Market, September 03, 2017, accessed March 10, 2017, https://ec.europa.eu/digital-single-market/en/cybersecurity.

[7] "Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace," Digital Single Market, February 07, 2013, , accessed March 10, 2017, https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace.

[8] Ibid

[9] "The Directive on security of network and information systems (NIS Directive)," Digital Single Market, September 03, 2017, , accessed March 15, 2017, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[10] Ibid

[11] "Cyber Security Strategy for Germany,", p 6

formally recognise the EUCSS and NIS-Directive, but also follow national interests external to the institutional strategy.[12]

The consequences of these double-paths have been noted as nation states attempting to establish digital borders within cyberspace through CS measures that seek to safeguard what these states refer to as the aforementioned national interests or sovereignty issues in cyberspace.[13] With this taken into account, the thesis aims to look at how the selected EU MS emphasise their own national interests over those enshrined in the EUCSS, which calls for all EU MS to cooperate under the CS initiative in question. There is also the factor of CS being seen as a capability to states.

In relation to the EUCSS, the cooperation initiative has been suggested to be obstructed in cases, where trust problems occur. That is, cases where MS hide certain information about their CS capabilities, because it is seen as a matter of sovereignty and national interests by these states.[14] These risks and threats have been cited as vague language in the documents pertaining to the EUCSS due to the supranational challenge of striking a balance between technical and political language in the strategy.[15] Other problems have been cited as weak implementation of the strategy due to the mix of voluntary and mandatory approaches in reporting on CS issues throughout the framework, and thus also the imbalanced enforcement of transnational CS in the EU.[16]

On the basis of the aforementioned observations, the thesis then seeks to analyse these problems facing the institutionalisation of European CS, and the obstacles to establishing a collective CS strategy. In order to analyse this problematisation, a pragmatic international relations theory approach is applied, together with established literature on CS, in order to contextualise the European CS problematisation into a greater context on CS and IR.

---

[12] Sarah Backman and Magnus Ekengren, *The Institutionalization of Cybersecurity Management at the EU-Level*, Master's thesis, Swedish Defence University, 2016 (Master's Programme of Politics & War), p 43
[13] Ibid, p 6
[14] Ibid, p 6
[15] Simon, Stephanie, and Marieke De Goede. "Cybersecurity, Bureaucratic Vitalism and European Emergency." *Theory, Culture & Society* 32, no. 2 (January 14, 2015): 79-106. Accessed February 4, 2017. doi:10.1177/0263276414560415, p 94
[16] Ibid, pp 23-24

Problem Statement

Thus the problem statement of this thesis is:

Why is it problematic for the European Cyber Security Strategy to establish a collective framework of cyber security?

Methodology

Research design

The epistemological position employed throughout the thesis works from the underlying logic of a pragmatic approach to international relations theory (IR). This type of approach has been recommended for the study of CS and its empirical cases, as it specifically addresses some of the entrenched positions between IR theories, for instance between realism and liberalism.[17] Thus, in relation to the analysis of CS strategies, this epistemological approach will offer a complementary approach to the analysis of the CS environment in these strategies. In this case, theoretical perspectives of realism and liberalism serve to offer complementary explanations for cooperation and conflict in CS. The pragmatic epistemological approach also seeks to bridge theory and practice, as well as seeking methodological pluralism through a combination of case study and comparative analysis. From this, further theory can be developed, with the basis on conditional generalisations instead of universal.[18] In relation to this thesis, this also means taking into account the intent and thereby practices of the object of analysis, specifically the MS and how these CS strategies are carried out. Thus it is also an attempt to look at the language-mediated aspects of these strategies, and how this informs the IR thereotical perspective.[19]

In order to analyse the CS strategies, a case study approach is applied in conjunction with

[17] Johan Eriksson, and Giampiero Giacomello. International relations and security in the digital age. London: Routledge, 2010., p 22-23
[18] Ibid, p 23
[19] Harry Bauer, and Elisabetta Brighi. *Pragmatism in international relations*. (London: Routledge, 2009.)

a comparative approach.

The case study is applied to the individual MS CS strategies, in order to assess how each strategy constitutes elements of liberal institutionalism, structural realism, and uses of cyber power as IR perspectives. The EUCSS is analysed from a liberal institutionalist perspective, in order to analyse how CS has become institutionalised. Based on these cases, the dimensions of cooperation and conflict can be established on the basis of the IR theories, and following this, the IR elements present in these strategies can be grouped into the dimensions. In doing so through a document-based analysis it is possible to analyse how these dimensions are present in each strategy i.e. how each CS strategy refers to cooperation through different IR approaches, and also how national CS strategies in some cases conflict with the overall EUCSS strategy in the conflict dimension. In the strategies, the IR perspectives are thus linked to policy provisions concerning international engagement on CS, national interests, sovereignty.

The thesis also utilises a comparative analysis approach, which helps contrast the selected cases. This allows for the setup of multiple observations in each case, through how each strategy refers to the cooperation and conflict dimensions, which can then be compared and contrasted in the analysis in relation to the main theoretical concepts employed in the thesis (CS, liberalism, realism, and cyber power). This can help explain similarities and differences in each national context.[20]

In connection with this, the IR perspectives can be linked to the CS literature in the theory, where it can then be argued that CS is contextual, whereas the IR perspectives expect states to behave rationally in a generalised manner. It can also be pointed out how states establish their own interpretations of CS in the context of the EUCSS. Thus the comparative analysis will also elucidate why the EUCSS faces the challenge of establishing a collective sense of security through CS in this engagement, through the comparative analysis of the individual cases.

Therefore, the research design also employs an interpretive approach to analysing CS in the backdrop of an IR theoretical approach, and how security has become a contested concept in the domain of CS. This will be linked to how the EUCSS uses its own interpretation of CS, and also how the MS bring their own interpretations. Thus, this phenomenon can illustrate how notions of CS have been taken for granted in international relations.[21]

---

[20] Alan Bryman, *Social Research Methods* (Oxford: Oxford University Press, 2012)., p 72

[21] Christopher K. Lamont, *Research methods in international relations* (Los Angeles: Sage, 2015)., p 43

Research Outline

In order to assess the dimensions of cooperation and conflict between the two cases of the EUCSS strategy and the national CS strategies, and thereby the degrees to the utilisation of liberal institutionalism and realism, as well as use of cyber power in the CS strategies, the analysis starts out by outlining the provisions related to national interests, sovereignty, and domestic/international cooperation in the selected documents. These provisions will be linked to both the liberal and realist theoretical perspectives through an analysis of the documents, detailing the core problematisations related to CS cooperation topics in the EU. The theory of cyber power will add an additional perspective to use of soft power in cyberspace.

Moreover, it will be possible to establish a theoretical argument for why CS and CS cooperation require a rethinking of the traditional IR theory - and therein take into account problematisations that have so far been neglected in the IR literature, as well as to establish the limits of IR theory in the CS strategies.

These problematisations will then be contrasted with alternative perspectives established by CS/information revolution literature, thereby illuminating alternative solutions to CS cooperation between MS and the EU institution. Finally this will lead into a discussion, where potential changes to the current interaction between MS and the EU supranational institutions related to CS cooperation can be suggested as alternative policy recommendations on how to overcome the current obstacles to cooperation in the EU context. This is based on the assumption that cooperation is the desired outcome between the MS and the EU, including its CS agencies.

Validity

The internal validity in the thesis is supported by the case study of the EUCSS, which specifically outlines the CS provisions related to cooperation mechanisms in the CS strategy, and the content is assessed The comparative analysis is matched with official reports from the EC and ENISA agency, where these areas of cooperation have been assessed and critiqued, and the secondary sources have also pointed out these issue areas, thereby supporting the causality of the issues raised between MS and the EU in CS cooperation.[22]

[22] Alan Bryman, *Social Research Methods*, p 47

The external validity is significant due to the balance of cooperation and conflict between MS and the EU have been pointed out in numerous cases, i.e. in official ENISA reports, academic literature, and MS government documents in relation to CS cooperation. Similar cases can be made for other existing CS cooperative engagements, which follow a similar logic of government and institution interaction, though there are exceptions to this type of framework in global security, such as the approach taken by the Shanghai Cooperation Organisation (SCO) which uses the definition of "information security."[23] Despite this, there is a degree of uniformity between a majority of institutions and their approaches in CS matters.

The results made in this thesis can be used when trying to gain a picture of how CS operates in Europe, and the institutions working in partnership with the EU. In addition, the research provides a study of the applicability of liberalism and realism, and how they operate as governance logics in CS cooperation initiatives, but also their limits. From this, policy recommendations can be made in domains that follow a similar logic of state and institution cooperation, and how this is reflected in their policymaking.[24]

Data collection

The research will utilise both primary and secondary sources. The primary sources will, on one hand, be in the form of official web documents as well as press releases from the European Commission and its associated agencies, such as The European Union Agency for Network and Information Security (ENISA), involved in drawing up the EU Cyber Security Strategy (EUCSS). [25] In addition, secondary sources and literature written on European CS will be utilised in the analysis of provisions related to cooperation in the EUCSS and NIS-Directive, as well as the individual national CS strategies. In doing so, web documents outlining national CS strategies of selected EU MS will be assessed and analysed, in order to find out how these particular national CS strategies align/and or diverge from the conceptualisation of CS in the

[23] "SCO," CCDCOE, September 07, 2015, , accessed May 2, 2017, https://ccdcoe.org/sco.html.
[24] Alan Bryman, *Social Research Methods*, pp 47-49
[25] "About ENISA," About ENISA - ENISA, June 24, 2016, , accessed March 12, 2017, https://www.enisa.europa.eu/about-enisa.

EUCSS and its legal basis, the NIS-Directive, outlined by the European Commission.[26] The EUCSS and the NIS-Directive will serve as contextualisation for the national CS strategies in the EU, as both the EU MS in the development of their CS plans.[27]

The EU MS selected for this analysis are Germany, France, and the U.K, as these represent some of the more powerful EU MS . The U.K, has also been taken into account, as it is a signatory of the EUCSS, and due to remaining a member of the EU internal market, and thus still a cooperative member of the NIS-directive as part of the overall EUCSS.[28]

From a thematic and interpretive basis, the aforementioned texts have been selected upon the criteria of their references to the topic of CS cooperation, both from the perspective of the EU CS, but also from the perspective of the EU as a supranational institution. This includes the agencies that are involved in the development of the CS strategy such as ENISA.

The secondary sources will then concern the actions that have been taken on behalf of the EUCSS and the national CS strategies of EU CS. Due to the multitude of current agreements and partnerships within the field of CS (some voluntary, some mandatory). In order to fully assess and critique CS cooperation in this context, it is also important to look at how EU MS and the EU itself have acted within each of their CS policy domains, and the extent to which these actions reflect discrepancies in relation to the official CS policies highlighted in the primary data.

Moreover, the secondary sources will also consist of books and journal articles that have dealt specifically with the development of the EUCSS and the implementation of national CS strategies of EU MS, but it should also be noted that the sheer number of actors involved in the processes of the EUCSS are delimited in the analysis to those actively engaged in the cooperative mechanisms of EU MS and the supranational institutions. In addition, there may be a variety of motivations for states to refrain from reporting on certain aspects of their strategies in the policy documents – as noted by ENISA's own report.[29]

---

[26] "The Directive on security of network and information systems (NIS Directive)," Digital Single Market, September 03, 2017, , accessed March 15, 2017, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[27] "Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace,"

[28] Ibid

[29] "Report on Cyber Crisis Cooperation and Management," Common practices of EU-level crisis management and applicability to the cyber crises, April 4, 2016, , accessed February 15, 2017, https://www.enisa.europa.eu/publications/eu-level-crisis-man.

The inclusion of secondary sources will thus add perspective and additional information to the analysis of the topic, dealing with similar problem areas to CS.

Finally, it should be noted that the source selection is based on availability of documents available to the public, and that getting full access to the details of each national CS strategy is unlikely, as some aspects of the strategies may be classified due to the fact that certain aspects of the national CS strategies pertain to classified national defense information or military capabilities within the cyberspace domain as touched upon earlier.

The development of the EUCSS is seen as an ongoing coordinated process with a wide variety of actors/stakeholders from both the private and public sectors, including working groups.[30] This factor provides an opportunity to focus the analysis on the intended cooperation aspects, as outlined in these strategies.

The selection of data in this thesis has been carried out through a qualitative methodological approach, based on its consideration of words rather than quantification of the data collection and the subsequent analysis.[31] Additionally, the primary documents have been selected on the basis that they serve as the original documents by individuals directly involved in drawing up the CS strategies. The secondary sources also reference and analyse aspects of the main CS strategies, which provides an additional perspective on the policies.[32]

Appendices of Cyber Security Strategies

Appendix 1: "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." - European Commission, 7 February 2013.[33]

This document serves as the main strategic outline of the European CS Strategy as well as a joint communication between the European parliament, the council, the European economic and social committee and the committee of the regions.

[30] Ibid, p 8
[31] Alan Bryman, *Social Research Methods*, pp 35-36
[32] Christopher K. Lamont, *Research methods in international relations*., p 80
[33] "Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace,"

Appendix 2: "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL" - European Commission, 6 July 2016.[34]
This document outlines the primary measures of the NIS-Directive, with the purpose of harmonising CS capabilities throughout the EU MS, including cross-border optimisation of information sharing and cooperation on matters related to CS.

Appendix 3: "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world." - United Kingdom, November 2011.[35]
This document details four strategic objectives of the UK CS strategy, covering both domestic and international objectives.

Appendix 4: "Cyber Security Strategy for Germany" - The Federal Government of Germany, February 23, 2011.[36]
This document covers ten strategic areas in the German CS strategy, and details framework conditions for its strategic output.

Appendix 5: "French National Digital Security Strategy" - Government of the French Republic, October 15, 2015.[37]
This document details five strategic objectives of the French CS strategy.

Limitations

Some of the limitations to this study relate to the nature of the document-based research undertaken in this thesis. While the documents analysed are authoritative and represent official stances on the policies in question, there are still problem areas such the research accessibility to the processes involved in drawing up these policies. One such example is the enormous scope of the coordination of the EUCSS, which involves a plethora of actors from the public sector to the private sector, as well as the multitude of policy arrangements preceding the current EU strategy

[34] "The Directive on security of network and information systems (NIS Directive),"
[35] "Cyber Security Strategy of the United Kingdom."
[36] "Cyber Security Strategy for Germany,"
[37] "France Cyber Security Strategy,"

on the matter.

Another limitation to this form of document based research is also the limited access to the social processes that have gone into drawing up the policies and official documents. Here it is recognised that interaction between actors in the policymaking process has been extensive. This could constitute another avenue of research on its own.[38]

In addition, while the data collected in this study has provided a comprehensive overview of the official policy stances between the EU and the MS, it is limited in respect to transparency of sensitive issue areas related to cyber defence. Some of these areas relate directly to the military capabilities of the MS which are not publically available. Therefore the data set is limited to what the MS have chosen to release to the public, which in most of the cases analysed, is the information sharing aspect of capability building in CS, and therefore also certain cyber defence intelligence provisions.

As an extension of this factor, there are still areas of these capabilities being developed in coordination with the ENISA Agency and other EU Commission Working Groups on CS. This also limits the analysis of these factors, for instance when assessing the willingness of MS to cooperate on these sets of capabilities, the limited development of the capabilities can be one explanatory factor for limits to cooperation.

Limits to the theoretical framework are also identified in CS being a relatively contested topic in international relations theory. However, this is also connected to the constant development and pace of technological innovations - especially in the area of communication technologies. This factor presents challenges to the textual analysis of the policy documents covering technical aspects of CS cooperation, as many of these are procedural processes and subject to change, thereby ultimately subject to policy amendments to a certain degree. Nonetheless, this limitation is taken into account on the basis of the data selection and the concepts defined in connection with the analysis of the data. The development of the EUCSS is also regarded as an ongoing coordinated process with a wide variety of actors/stakeholders from both the private and public sectors, including working groups.[39] This factor provides an opportunity to focus the analysis on the intended cooperation aspects, as outlined in these strategies.

[38] Ibid, p 82
[39] "Report on Cyber Crisis Cooperation and Management,", p 8

Literature Review

In this section, the aim is to provide an overview of the established literature on CS and how it has previously been applied as a concept in relation to cooperation and conflict surrounding this concept. This also covers CS literature in the context of the EU. In this regard, this section also considers concepts related to CS, and where cooperation has been sought by states and institutions alike. In this connection, the aim is to touch upon literature covering concepts such as "cyberspace", "information society", "information security" and "cyber power" "information revolution", and assess their linkages to the contemporary CS debate. It is through an understanding of how these concepts have evolved in academic literature, and specifically in IR that it is possible to build a theoretical framework informed by these concepts.

Furthermore this opens up for an in-depth critique of how the EU and EU MS utilise the concepts of CS and CS cooperation, and moreover, how specific provisions in the EUCSS outlines its provisions for CS cooperation. In order to assess how this dynamic has been covered in the information revolution/CS literature, this section will be divided into two chapters of cooperation and conflict. The following section will cover concepts related to institutional and societal aspects of CS cooperation.

Bossong and Wagner have criticised the concept of "cybersecurity" as two individual concepts containing both "cyber" and "security" and arguing that it has been incorrectly used by CS institutions under the EUCSS framework. due to their wide applicability in both contemporary society and human life.[40] Tropina and Callanan have in this connection also noted how there is no specific internationally accepted definition of CS. Not within the EUCSS framework, or similar engagements in this field. [41] However, there has been a variety of academic attempts to conceptualise what exactly CS entails prior to this specific discussion of the EU experience.

One of the earlier examples of this is the information society literature, where Manuel Castells has focused on the development of industrialised economies to network societies in

[40] Bossong, Raphael, and Ben Wagner. "A typology of cybersecurity and public-private partnerships in the context of the EU." *Crime, Law and Social Change*, 2016, 1-24. doi:10.1007/s10611-016-9653-3., pp 19-20

[41] Tatiana Tropina and Cormac Callanan, *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security* (Cham: Springer International Publishing, 2015)., p 9

which addresses the role of the market and non-state actors. Moreover, this literature primarily concerns itself with the role of non-state actors and the market in the information society, rather than addressing the role of CS, and whether it even serves as a problem to states or institutional actors specifically.[42] While important to the discussion, it also does not address the governance tools that are available to state and non-state actors. On the contrary, this work provides an important contextual purpose for theorisation of the information society as an extension of industrialised economies. The focal point of Castell's argument is the increasing importance of information as a resource in what is referred to as an "information economy."[43]

In this connection, Castells points to the fragmented role of the state and its decreased sovereignty, as these non-state actors in charge of crucial services become crucial to the continued function of modern societies.[44] The work is still important for understanding how information has become intrinsically tied to all services in modern society. In this sense, the work does touch upon security in relation to information, but it is primarily concerned with information security in relation to organised crime, the military sector, and information as propaganda.[45] Therefore the information society literature is limited when trying to analyse the ramifications of institutionalised CS in the EU, and thereby also how cooperation takes place in this field. On the other hand, it provides important insight into the role of technology in modern society.

On the other hand, scholars such as Eriksson and Giacomello have sought to address the lack of International relations theory to the field of CS. Here they argue that previous IR theories have not taken the impact of the information revolution into account in relation to IR theory. [46]

In their review on past literature on what they call the global information society, they find that the literature has primarily focused on the security of markets and firms, rather than the security implications for the state and society.[47] In doing so, they advocate for mixed middle-range theories that utilise concepts in liberalism, realism, and constructivism as they argue that

[42] Manuel Castells, *The Informational city: Economic restructuring and urban development* (Oxford: Basil Blackwell, 1989).
[43] Ibid, p 126
[44] Manuel Castells, *The Informational city: Economic restructuring and urban development*
[45] Ibid

[46] Johan Eriksson and Giampiero Giacomello, *International relations and security in the digital age* (London: Routledge, 2010), p 3
[47] Ibid

the impact of the information revolution on security is multifaceted and involves both multiplicity of non-state actors from a liberal perspective, but also threat representations of cyber-attacks from a constructivist perspective, and information warfare from a realist perspective, which also looks at CS as a capability.[48] Thus this pragmatic approach elucidates the gap in CS studies with IR theory and makes it possible to use this approach to analyse the impact of the information revolution on IR studies, and also establish a link of interaction between CS and state and non-state actors.

While the aforementioned approach tells us something about the general coordination efforts of CS and the interaction between state and non-state actors plus the importance of socially constructed ideas in CS. It, however, does not further elaborate on the EU specific approach to CS and attempts to institutionalise CS through a particular governance logic through interaction between private and public sectors.[49]

Backman, in her thesis, has analysed the institutionalisation process of European CS through the theoretical lens of a neo-functionalistic approach. In this she notes that while the institutionalisation process has taken place through a cultivated spillover process, where a majority of EU MS have welcomed CS measures, there are still cases, such as Britain, France, and Germany who have developed so-called double-paths and essentially refer to their own CS strategies as the primary concern, and thereby their interests in this domain as their priority.[50]

In this case, it would be appropriate to turn to scholars such as Christou who approaches CS in the EU from the concept of "cyber resilience."[51]

The idea of resilience is a concept which is reiterated in the EUCSS framework, and concerns the ability to recover from a multitude of cyber-attacks that target critical infrastructures and information sensitive sectors of society. The theoretical explanation serves as a useful tool to explain the governance logic of CS in the EUCSS, and also how states implement their national strategies in coordination with this logic of security as resilience utilised by the EUCSS.[52]

---

[48] Ibid, p 22

[49] Appendix 1, p 14

[50] Sarah Backman and Magnus Ekengren, The Institutionalization of Cybersecurity Management at the EU-Level, Master's thesis, Swedish Defence University, 2016 (Master's Programme of Politics & War), pp, 43-44

[51] George Christou, *Cybersecurity in the European Union* (Basingstoke ; New York: Palgrave Macmillan, 2016)., p 1

[52] Ibid, p 187

The concept of resilience has also been covered in the context of the national CS strategy of the U.K by Herrington and Aldrich. The two scholars point out how the limits to the current model of resilience in the U.K CS strategy in which this approach mirrors the EU's conceptualisation of resilience. The criticism is aimed at the overlap between the public and private sectors in the UK National Security Strategy in which the main provisions of the strategy are kept secret, yet also call for cooperation between these two sectors, where information sharing becomes part of the resilience logic.[53]

In addition, Herrington and Aldrich point out that European CS agencies such as ENISA experience similar problems to national governments when it comes to cyber-resilience. These problems occur because on one hand, the governments and institutions design CS projects that are grand in scope (referred to as "big-bang solutions"[54]), but the private sector moves at an accelerated pace due to the constant development of technologies, and especially ICT related technologies.[55]

This can also be related to the EUCSS framework, which calls for increased use of public-private-partnerships between MS and the EU CS authorities. However, as will be shown in the empirical section, this also becomes problematic when states insist on keeping particular provisions of their CS in line with their own approach to how information sharing takes place in these provisions. In the selected cases, these are provisions related to national interests and sovereignty.

Cavelty, Kaufmann, and Kristensen have analysed how the multitude concepts and practices of resilience have often been used in contradictory ways in security studies, and moreover, how these issues have been present in several domains, ranging from military programs to critical infrastructures.[56] The idea is that resilience exists in different temporalities, and often acts as a reaction toward problems in the past and future. This leads to the idea of resilience as something that exists in the past and future but not in the present.[57]

---

[53] Lewis Herrington and Richard Aldrich, "The Future of Cyber-Resilience in an Age of Global Complexity," *Politics* 33, no. 4 (2013): , accessed April 1, 2017, doi:10.1111/1467-9256.12035, p 301
[54] Ibid, p 304
[55] Ibid
[56] Myriam Dunn Cavelty, Mareile Kaufmann, and Kristian Søby Kristensen, "Resilience and (in)security: Practices, subjects, temporalities," *Security Dialogue* 46, no. 1 (2015): , accessed March 15, 2017, doi:10.1177/0967010614559637.,p 4
[57] Ibid, p 9

This also leads to the question of the concept of resilience as a point of cooperation in CS strategies between MS and the EU, where a variety of security concerns are at play in both the past, present, and possibly future for the individual MS and the EU. Therefore this problemisation of cooperation in CS also relates to the different understandings of CS at an institutional and MS level. In this connection, Simon and de Goede have looked at CS in the EU from the perspective of what they call "bureaucratic vitalism" and "European emergency." The former concept relates to the EU attempts to balance supranational security apparatuses on one hand, and establishing resilient networks through CS agencies and information sharing groups.[58]

From this point we can move into the conflicts surrounding CS, and how these conflicts might be tied to the implications for CS cooperation. In this regard, we can for instance look at how states approach threats in cyberspace, and how this leads them to formulate CS approaches or cooperation initiatives. Deibert and Rohozinski divide cyberspace security into two realms of "risks."

They essentially argue that these risks affect the extent to which these states are willing to engage in CS cooperation.[59] In this they make a distinction between two types of risks related to CS. The first is risks to cyberspace itself. That is, risks to the actual communications technologies that are connected to cyberspace through for instance critical infrastructures, which both public and private industries rely on.[60] The second sets of risks are those coming through cyberspace in the form of easily accessible media use and instant communication by use of social media platforms.

Deibert and Rohozinski elaborate on the attempts to secure cyberspace and how the two different risks affect the outcome. In sum, the authors argue that these risks to cyberspace have led to a growing international consensus that recognises the importance of economics, private and public sectors, and the need to secure commerce and infrastructure through cyberspace.[61]

---

[58] Simon, Stephanie, and Marieke De Goede. "Cybersecurity, Bureaucratic Vitalism and European Emergency.", p 79

[59] Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010): , doi:10.1111/j.1749-5687.2009.00088.x.
, p 15

[60] Ibid, pp 18-19

[61] Ibid, p 29

On the other hand, risks through cyberspace create a contentious debate among states, as these states are insisting on national policies and approaches where the state insists on self-reliance in CS.[62] These policies thus create insecurities in cyberspace when states insist on surveillance and filtering measures against risks through cyberspace, while also insisting on a frictionless cyberspace in the risks to cyberspace, thus creating a paradox between these two risk approaches.[63]

The aforementioned literature informs about the multiple, and how it also creates implications for CS cooperation when states insist on safeguarding themselves from certain risks from cyberspace, particularly in regard to their own national interests. At the same time, the authors also show how risks to cyberspace are managed by private actors and even non-state actor activities, and therefore a crucial element of CS frameworks.[64]

Thus the authors also conclude that the paradox created in CS does show what they call a "return of the state", however not in the form of the Westphalian paradigm due to the dynamic of states trying to limit and shape cyberspace in their interests, but also private and non-state actors who create these technologies or circulate information for their own reasons.[65] This literature may help explain instances where the state wants to secure things from cyberspace, but also support a cyberspace which supports their economic and political motivations.

Other CS literature has also touched upon state power and its implications for CS and cooperation. Demchak and Dombrowski essentially argue that ICT technologies have led to the rise of a "cybered westphalian age."[66] With this concept, the authors argue that because cyberspace is man-made, this also allows for the establishment of borders in cyberspace, where states will take increasing steps to secure against threats coming through cyberspace.[67]

The authors cite examples of these border-making processes in cyberspace, with China as an example, but also the EU due to the fact that MS have their own national CS policies.[68]

---

[62] Ibid, pp 29-30
[63] Ibid, p 30
[64] Ibid, pp 29-30
[65] Ibid, p 30
[66] Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age: The Coming Decades," *Strategic Studies Quarterly* 5, no. 1 (2011): , doi:10.1007/978-3-642-55007-2_5., p 32
[67] Ibid, pp 34-35
[68] Ibid, p 47

It also mentions the U.K as an example of laying the foundation for a cyberspace national border. Considering the efforts by the U.K to influence policymaking in the EUCSS framework[69], there is an argument to be made in this context.

Ultimately, the authors see the consequences of the cybered westphalian age phenomenon in relation to CS cooperation, due to international norms that will have to be negotiated "state by state, region by region."[70] Because of the coordination challenges and time it takes to build international regimes around cyberspace, the authors contend that states will first and foremost seek to control how cyberspace affects their citizens and their own interests. In addition, the authors contend that as states build up their borders in cyberspace, national laws of states will be the rule, and attacks across these cybered borders will also become the responsibilities of the different states.[71]

One may also relate this factor to the institutionalisation process of the EUCSS, where EU MS had already established their own CS policies, where they cite concerns of national sovereignty and national interests and viewing cyber-attacks as a threat to their sovereignty.[72] However, the literature is also not sufficient in explaining why states then both acknowledge international regimes such as the EUCSS, and even openly support these initiatives in their own strategies, while also emphasising their own national interests in CS. In this regard, it is appropriate to explore literature on why states then insist on asserting their interests through cyberspace and CS cooperation. This also looks at how these states make use of CS as a capability and something that can be wielded, similar to a tool of statecraft.

In doing so, several of them have analysed this factor through the lens of what they call "cyber power."[73] Klimburg sets out to analyse how states can project power in cyberspace and goes on to provide a model for how cyber power encompasses both state and non-state actors. In this, he argues that states who seek to exercise power in this domain will have to either co-opt or coerce the non-state sector of society to cooperate with the state.

---

[69] George Christou, *Cybersecurity in the European Union* (Basingstoke ; New York: Palgrave Macmillan, 2016)., p 80

[70] Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age: The Coming Decades,", p 55

[71] Ibid, p 57

[72] "France Cyber Security Strategy,", p 17

[73] Alexander Klimburg, "The Whole of Nation in Cyber Power," *International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity*, 2011, , accessed March 29, 2017, http://www.jstor.org/stable/43133826., p 171

The result is the "Integrated Capability Model of Cyber Power" approach that incorporates civil society and the private sector as they are part of the non-state sector which maintains and operates the majority of the internet infrastructure.[74] Thus, the argument is that states must attain cooperation with these two sectors in order to efficiently exercise cyber power.[75] It can be argued that this model also provides a counterpoint to realist approaches in cyberspace and topics of CS, as Klimburg evidently shows that states must seek cooperation with these sectors in order to exercise their own state power through a form of soft power.[76]

Klimburg also stresses that the most important dimension for states is to establish cooperation with non-state actors and thus create a "whole of nation" CS policy approach that specifically seeks to cooperate with non-state actors that run internet services vital to the CS of the state, and effectively outside state control.[77] Empirical examples of this type of soft power, is for instance seen in Britain, where the "Centre for Protection of National Infrastructure" is tasked with protecting British industries from cyber-attacks.[78] Other approaches to cyber power have also taken instruments of cyber power into account.

Nye presents a wide definition of cyber power as "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[79] Nye's conceptualisation of cyber power also makes a distinction between physical and information instruments. Both of these instruments can be utilised by a state to project power inside and outside cyberspace. One such example is how information instruments inside cyber space can be used to set agendas or persuade software developers to follow certain standards set by the state.[80] In terms of hard power inside cyberspace, this could be the utilisation of cyber resources by state and non-state actors, with the purpose of targeting systems or critical infrastructures of rival actors/states.[81]

---

[74] Ibid, p 174
[75] Ibid, p 176
[76] Ibid, p 177
[77] Ibid
[78] Alexander Klimburg. "Mobilising Cyber Power." Survival 53, no. 1 (January 28, 2011): 41-60. Accessed March 28, 2017. doi:10.1080/00396338.2011.555595., p 52
[79] Nye, Joseph S. Cyber power. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010., p 4
[80] Ibid, p 5
[81] Ibid

In sum, Nye contends that cyber power is utilised by both state and non-state actors, but with the caveat that non-state or smaller actors may benefit more from this power. Thus leading to asymmetrical vulnerability due to the low investment from the smaller attackers, who carry out these attacks, and the high potential damage to critical infrastructure of states and corporations.[82] From Nye's point of view, cyber power is therefore also a form of diffusion of power leaning towards non-state actors, despite the fact that governments are still in control of the physical infrastructure of the internet through geography, and can therefore encourage or discourage development of cyber capabilities inside their borders.[83] Overall, this idea of cyber power calls for cooperation between the state and non-state sectors, if cyber power is to be wielded by a particular government. Yet it also challenges the presumption that the state solely resides over this domain as with other military domains.[84]

Cavelty has sought to analyse how national security in cyberspace have become securitised and thus how CS is presented as a national security issue.[85] In doing so, Cavelty looks at different discursive threat representations in CS discourse. This includes the understanding of discursive practices of state and non-state actors in CS, grants an understanding of the choices available to these actors, and how this affects CS policies.[86] The interesting point made by Cavelty is how discursive representations of CS are treated as a contentious area by a variety of state and non-state actors, who each provide their own interpretations of threat representations in CS discourse.[87]

From this point, Cavelty argues that two dominating logics are currently conveyed through threat representations and practices in CS. The first one refers to discourse that links cyberspace and the need for the state to establish borders and order through CS practices. As this discourse becomes more directed at the need for borders and control in cyberspace, the more actual critical infrastructures can have principles of sovereignty and territoriality imposed on

[82] Ibid, p 13
[83] Ibid, p 9
[84] Ibid, p 19
[85] Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review* 15, no. 1 (March 2013): , accessed March 20, 2017, doi:10.1111/misr.12023., p 105
[86] Ibid, pp 105-106
[87] Ibid, p 118

them.[88] The second logic is concerned with CS as an organic process, capable of self-organisation, through interconnected networks. The problem is that these two logics are conflicting as they paint two different pictures of cyberspace as an untamed place, but also as an "auto-generating immune force."[89] Thus, this leads to two scenarios. One where the state is a facilitator in CS, and one where the state must interfere in the global setup of cyberspace/the internet.[90] Cavelty notes that threat representations have so far focused on the second logic, which has led to CS being treated as a military issue, where military actors must intervene and secure cyberspace from threats.[91]

Although this theory deviates from the previously mentioned theories through a semi-constructivist perspective, it arguably serves as a valuable insight into why states make certain decisions related to CS and cooperation therein. One of the important criticisms made by Cavelty in this text, is when she notes the lack of IR theory application in the field of CS studies.[92] In this she also refers back to the previously mentioned scholars Eriksson and Giacomello who have made similar criticisms.[93] It is also interesting to point out Cavelty's argument that non-state actors, such as technological experts have had a significant discursive effect in how CS political agendas are constructed.[94]

The insight gained from this theory is valuable to this study of CS cooperation in the EU, as it provides a theoretical link to the CS debate. Moreover, it provides an in-depth analysis of how CS is discursively linked to questions of national security by EU MS.[95]

Sub-conclusion: Literature Review

The aforementioned literature thus informs the CS debate by highlighting different issues that have been raised in relation to cooperation and conflict in CS. From this it becomes apparent that there exist different interpretations of CS, where on one hand, it is seen as a crucial function of modern society e.g. through maintenance of critical infrastructures and non-state cooperation. On

[88] Ibid
[89] Ibid, p 119
[90] Ibid
[91] Ibid
[92] Ibid, p 106
[93] Ibid
[94] Ibid, p 118
[95] Ibid

the other hand, it has also been framed as a military issue and capability, connecting territoriality and sovereignty to cyberspace. However, it has also been framed as an economic good from a liberal perspective. Finally, cyber power also shows measures of soft-power and hard-power that can be used in the domain of cyberspace.

Central themes in the CS literature	**Cooperation**	**Conflict**
CS/information revolution literature	- Resilience as security - Risks from and to cyberspace leading to international consensus on CS - Critical infrastructures as a crucial element of CS cooperation - Non-state sector as provider of technologies - Information economy - CS as essential to industrialised economies	- CS as a national security issue - CS as a military issue - Threats from cyberspace - Limits to information sharing - Contradictory applications of resilience (past and future) - Securitisation of cyberspace - Territoriality - Contentious representations of threats in cyberspace - Double-paths
International relations theory	- Liberalism: instituionalised CS, inclusion of non-state actors, civil society,	- Liberalism: CS as an economic issue - Realism: Information warfare
Cyber Power	- Cyber power as cooperation between state and non-state actors - Cyber power as soft power in institutions	- Cyber power as hard power - Cyber power as an instrument of power - Challenges the state

Theory

The purpose of this section is to outline theory which will investigate the phenomenon of CS cooperation in the context of the European CS Strategy of 2013. More specifically, it will look at how the phenomenon of the MS of Germany, France, and the UK, and whether these deviate from the EUCSS in their own national CS strategies, and how this can be explained from the following theories.

There is a noticeable gap in the literature on international relations theory, in explaining how the dynamic in CS cooperation and conflict occurs between states. It is argued that the liberalism and realism strands of IR theory have previously not informed each other on the issue of security in cyberspace.[96] Furthermore, it has been suggested that a pragmatic approach can be operationalised to alleviate some of these issues, with the purpose of overcoming some of the polar oppositions in IR theory.[97]

On the other hand, literature on the information revolution, such as cyber power takes into account the tools available to states in cyberspace and how they can utilise these statecraft tools, in order to engage with a wide variety of non-state actors and institutions in CS cooperation.[98] However, it does not analyse the factor of cooperation and conflict in CS cooperation. Moreover, the approach is limited in explaining why actors make certain decisions in CS cooperation. Instead, the theory is more oriented towards the means available to an actor in cyberspace.[99]

The additional perspective of cyber power allows for an analysis of how actors utilise power in cyberspace, and thus through which measures power is negotiated in CS cooperation. Therefore cyber power serves the theory for contextual purposes, and the theory can then be linked to the framework of liberalism and realism.

---

[96] Johan Eriksson and Giampiero Giacomello, *International relations and security in the digital age* (London: Routledge, 2010), p 22

[97] Ibid, p 23

[98] Alexander Klimburg, "The Whole of Nation in Cyber Power,"

[99] Jelle Van Haaster, "Assessing cyber power," *2016 8th International Conference on Cyber Conflict (CyCon)*, 2016, accessed April 13, 2017, doi:10.1109/cycon.2016.7529423., p 15-16

From this position, it will be possible to show EU MS combine liberal institutionalism and neorealism/structural realism in the international sphere of CS cooperation. This serves to define the cooperation dimension. The conflict dimension serves as a secondary unit of analysis to highlight the gaps in the cooperation dimension, and provide an explanatory dimension to the problematisations in the European approach to CS

In addition, the inclusion of the combined liberal and realist approaches overcomes some of the criticisms that have been aimed at the study of the information revolution and overemphasis on what has been described as "technological determinism." - in doing so, some scholars have attributed the idea of constant progress to emerging technology, while ignoring other factors such as the role of security and its role in the information age.[100] The idea proposed here is to look at the political nature of CS, rather than technological aspect that neglects the role of private and public actors in the political process and consensus building within CS cooperation.

Therefore the aim of this section is to provide a pragmatic theoretical framework constructed out of the aforementioned theories, with the purpose of applying it to the analysis of the supranational coordination challenges within the EUCSS framework, and why the selected states engage in CS cooperation initiatives, but also provide an in-depth analysis of the empirical cases where the selected states divert from the mentioned initiatives and the factors that are involved when states make the decision to follow their own national CS strategies, and the extent to which these strategies disrupt the supranational CS cooperation initiatives.

The relevance of Liberalism in CS

The first point to make is to make sense of cooperation from the perspective of liberal international relations theory. In this regard, the theory begs the question why states engage in cooperation initiatives. Having noted that the EUCSS involves initiatives across the public and private sectors, nationally and transnationally, but also national CS strategies, with their own

[100] Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia. Krishna-Hensel, *Power and security in the information age investigating the role of the state in cyberspace* (Aldershot, Hants, England: Ashgate, 2007)., pp 20-21

domestic interests in cyberspace; it thus leads to the question of how liberalism can explain CS as a cooperative engagement.

In the basic definition, Baldwin divides liberal theory into three major terms of liberalism. In the first, we find commercial liberalism, which deals with the theoretical linkage between notions of free trade and peace. The second being republican liberalism which links the concept of democracy to peace. In the third label, we find sociological liberalism which links transnational interactions with the notion of international integration.[101] It is from these three points neoliberal institutionalists divert into their own framework of liberal institutionalism.[102]

In terms of contributions made by liberalism to IR theory, four significant contributions have been highlighted in scholarship. The first relating to the plurality of international actors, which is for instance evidenced in the environment of CS. Secondly, domestic political factors are deemed important determinants of how states behave internationally. Third, the role of international institutions and how they establish certain rules of behaviour.[103] (This can can be reflected in the EUCSS, in how it seeks to establish a certain type of behaviour in CS, as covered earlier.) Finally, the creation of subfields in IR studies, such as international political economy by adding more issue areas to the agenda can also be considered a significant contribution.[104]

Having set the foundation for liberal IR theory, it is then possible to suggest a liberal theoretical framework that reflects the environment of CS. In this connection, it would be appropriate to approach liberalism in CS cooperation from that of a liberal institutionalist and complex interdependence framework, as it will help describe the cooperation between the selected MS and the EU, and furthermore, how this can be adapted to an environment of where cooperation revolves around information technologies.

The primary argument made by liberal institutionalism is that international institutions now hold the primary role in international relations.[105] In addition, these institutions are capable

---

[101] David A. Baldwin, *Neorealism and Neoliberalism: The Contemporary Debate* (New York: 1993), p 4

[102] Ibid

[103] Johan Eriksson and Giampiero Giacomello, " The Information Revolution, Security, and International Relations: (IR)relevant Theory?," *International Political Science Review* 20, no. 3 (2006):, accessed April 2, 2017, doi:10.1177/0192512106064462.,p 229

[104] Ibid

[105] Robert O. Keohane and Lisa L. Martin, "The Promise of Institutionalist Theory," *International Security* 20, no. 1 (1995): accessed April 15, 2017 , doi:10.2307/2539214.,p 45

of facilitating cooperation in complex situations, where several states are involved.[106] It can be argued that this point reflects the environment of CS cooperation in the EU as it is a situation where several national CS strategies must be taken into account, while the role of the EC, ENISA agency and other CS agencies is to facilitate CS cooperation in coordination with the MS. From this perspective, the EU as an institution is the primary facilitator of CS in Europe. However, the EUCSS also recognises that it is the primary responsibility of states to establish their own CS strategies. Despite this, the coordination of CS is controlled by the aforementioned institutions.[107]

In connection to liberal institutionalism, institutions are also seen as capable of providing information about distribution gains among states in a cooperative initiative through institutions, and thus also reassure states against fear of cheating and unequal gains in cooperation initiatives. This information also relates to security issues, as it can disclose specific information about military capabilities.[108] Therefore, it has also been noted that institutional information can provide states with information of both political-economic relationships, but also those based on military-security.[109]

In the CS discussion in the EU, the institutional role would for instance be to facilitate information sharing of CS capabilities between MS, and for the ENISA agency to ensure communication lines between public and private sectors among the MS.

An important aspect of this is the notion of reciprocity as a crucial element in international institutions, where states cooperate and share information.[110] The strategy of reciprocity asserts that states abiding by this strategy through cooperation exchange information among one another, and therefore are concerned about the value of the information exchange.[111] The point made about the notion of "institutionalized reciprocity" is that reliable information is a requirement for states to willingly engage in cooperation in an institutional setting and effectively achieve absolute gains within this system.[112]

---

[106] Ibid
[107] Appendix 1, p 4
[108] Robert O. Keohane and Lisa L. Martin, "The Promise of Institutionalist Theory,", pp 45-46
[109] Ibid, p 43
[110] Ibid, p 46
[111] Ibid
[112] Ibid

This is reinforced by the logic of absolute gains in liberal theory, which asserts that states engaging in institutions are primarily concerned with absolute gains. Meaning that a state is not concerned with the relative gains of another state, but rather that cooperation leads to an absolute gain.[113] This effectively means that the state in an international institution is concerned with the absolute level of economic welfare that it can achieve within this institution, and not the relative gains it can achieve over other states.[114]

It is from this point, this theory can be linked to the experience of the EUCSS. This is seen in how MS have willingly ceded part of their sovereignty over CS issues through information sharing with the ENISA agency and the European Commission. This in itself, should reassure and inform the national CS strategies, provided the information is adequate. The MS would therefore receive reliable information about what this form of institutionalised CS entails.

Bridging the gap between Liberalism and the CS literature

While the liberal institutionalist theoretical lens can help capture the environment of institutionalised CS, there is still a need to elaborate upon liberalism in connection with CS and how exactly liberalism connects with the concept of security in CS. In addition, liberalism has been criticised for not taking security into account in its criticism of a realist interpretation of security.[115]

Despite these limitations, it is still possible to move liberalism into the CS debate. Eriksson and Giacomello have pointed out two contemporary socioeconomic trends that reflect the environment of CS in liberal democracies, and thus the relevance of liberal IR theory in this debate. One of these is the increasing trend of partnerships between private and public sectors to provide services, and the other the increased merging of civil and military areas in the digital age.[116] In this connection, it has also been suggested by Cavelty that the information age/digital

[113] Robert Powell, "Absolute and Relative Gains in International Relations Theory," *The American Political Science Review* 85, no. 4 (1991): , accessed April 12, 2017, doi:10.2307/1963947., p 1303
[114] Ibid, p 1305
[115] Johan Eriksson and Giampiero Giacomello, *International relations and security in the digital age*, p 231
[116] Ibid

age and increased range of transnational non-state networks have fragmented the monopoly on authority previously held by states.[117]

This has effectively led to a process in which both public and private governance structures undermine the authority of the state.[118] Finally this results in blurred lines between the state and the private sector in terms of capacities and responsibilities due to the multiplicity of actors involved in the policymaking process.[119] As a consequence, this has led to a multistakeholder approach when governments attempt to secure the ramifications of the information age, as many of the critical infrastructures and information are under control and ownership by the private sector. [120]

For this reason, any threat through cyberspace aimed at these systems will then carry consequences for both the state and the operators of these infrastructures. Moreover, because the critical infrastructures are largely owned by the private sector, they carry the primary role of securing these systems, and therefore also carry a significant influence on any protection measures for these systems in relation to CS.[121]

These measures often carry over between national and international security. Therefore it becomes clear that the information age consists of several key actors who can influence policies related to security of the state, but also transnational security issues.[122] However, it is also emphasised that governments cannot tackle these issues in CS alone, and thus the entire process of policymaking has to draw in multiple entities, including state and non-state actors.[123]

In relation to the EUCSS, these factors can be pointed out as the proliferation of PPPs in order to establish trust between states and private actors as a means of establishing CS.[124] Moreover, the blurred lines between military and civil domain is highlighted by the EUCCS provisions seeking to upgrade cyber defense between MS through information sharing across private and public sectors.[125]

---

[117] Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia. Krishna-Hensel, *Power and security in the information age investigating the role of the state in cyberspace*, p 32
[118] Ibid
[119]Ibid
[120] Ibid, pp 32-33
[121] Ibid, p 33
[122] Ibid
[123] Ibid, p 32
[124] Appendix 1, p 17
[125] Ibid, p 11

In choosing a liberal theoretical approach that takes the aforementioned factors into account, one can point to the theory of complex interdependence introduced by Keohane and Nye. The revised edition of this theory seeks to address some of the challenges presented by the digital age.[126] This also makes it relevant as a tool to analyse CS from a liberal perspective as it describes the costs of interdependence as an amendment to the theory of complex interdependence.[127] In addition, it is an attempt to integrate the notion of the information revolution with complex interdependence and thus outline a theoretical stance based on these principles.

Complex Interdependence

Keohane and Nye outline the basic notion of complex interdependence as a system through three defining characteristics. The first relates to multiple channels of contact between societies, where the state is not the sole provider of contact between societies. Instead, it is argued that these multiple channels connect societies, whether through transnational organisation or informal ties between non-state actors or governmental elites.[128]

The importance of these actor activities is observed in how they can influence policies in two ways. These actors are capable of increasing the sensitivity of government policies between two countries. This takes place due to the widened scope of domestic government activities, and because the private sector now makes decisions that go beyond the national borders of a government.[129] All of these factors are strengthened by transnational communications, which leads to increased activity between foreign and domestic policies, but also by turning more issues into foreign policy. Regulations tied to technological development serves as an example of this trend.[130] It can especially be argued that CS is pertinent to this issue, due to its embedded transnational communication between institutions and states, and how private actors make

[126] Johan Eriksson and Giampiero Giacomello, *International relations and security in the digital age*, p 231
[127] Ibid
[128] Robert Owen. Keohane and Joseph S. Nye, *Power and interdependence* (Boston: Longman, 2001).,p 21
[129] Ibid, p 22
[130] Ibid

decisions that go beyond the domestic level.[131] These channels can also be seen as a set of transnational relations.[132]

The second characteristic defines the absence of hierarchy among issues as interstate relationships not having a clear hierarchical set of issues, but rather multiple ones that become blurred between domestic and international issues.[133] For instance, military security is not always on the agenda.[134]

The third characteristic describes the decreased role of military power in complex interdependence. This can be observed by how the use of military force is only reserved for situations where complex interdependence cannot resolve the situation, such as the immediate survival of the state. However, these situations are unlikely, and in the end, the state is priorities goals of economic gain. On the other hand, this also asserts that if economic interests of a state are threatened by military power, then the realist assumptions of military force as a response can be valid.[135]

The purpose of the aforementioned characteristics is thus how they all lead to three specific political processes where power resources can be translated into the power to control outcomes.[136] The first of these are referred to as linkage strategies. This suggests that because there is no specific hierarchy of issues in complex interdependence, state goals will be dependent on the issue at hand. This also applies to the distribution of power and the political processes related to the specific issue.[137] States primarily focusing on military dominance will face difficulties when using force in issue areas where they show weaknesses. Similarly states using purely economic power may also face problems, as economic objectives have political ramifications and are ultimately tied to both domestic, transgovernmental, and transnational actors with their own interests and different sets of issues.[138]

Because of the negligible role of force in complex interdependence, the linking of issue areas becomes more problematic, which leads to states with low vulnerability to use international

[131] Ibid
[132] Ibid, p 21
[133] Ibid
[134] Ibid
[135] Ibid, pp 23-25
[136] Ibid, p 24
[137] Ibid
[138] Ibid, pp 24-25

organisations and transnational actors, as well as communication flows as a form of asymmetrical interdependence. Economic interdependence will be used by states as a source of power, and to take considerations for its citizens in terms of welfare.[139]

Agenda setting is the assumption that due to a clear hierarchy of issues, the politics of agenda formation and control will become even more important in this system of affairs.[140] Domestic forces will be able to push issues to the forefront of the interstate agenda and also politicise issues that would otherwise not end up here.[141] Governments with increasing strength can politicise certain issues through the linkage to other issues. International regimes may be affected by this, and domestic groups may attempt to influence interstate bargaining at this level to suit their interests.[142]

Transnational and transgovernmental relations make up the third condition of complex interdependence. Transgovernmental coalitions can be created through the multiple channels of contact, where governments through government agencies can bring in actors from other governments and establish alliances on decision-making processes.[143] Because of the multiple channels of contact, the line between domestic and international politics becomes increasingly difficult to distinguish between. This essentially limits statesmen in their manipulation of interdependence and ability to follow a "consistent strategy of linkage."[144] Moreover, national interests become more difficult to define on different issues, and with different actors, time, and governmental units.[145]

It should be noted that Keohane and Nye use this model to explain regime change. However, the concepts used in "complex interdependence" can arguably just as well be adapted to European CS, and used to explain the political processes taking place between state and non-state actors at both the domestic and institutional/international level. In addition, it can also serve as a contrasting theory to the later applied realist approach. Complex interdependence is in this regard also contrasted with realism, and each serve different explanatory purposes, depending on

[139] Ibid, p 25
[140] Ibid, pp 25-26
[141] Ibid, p 26
[142] Ibid
[143] Ibid, p 27
[144] Ibid
[145] Ibid, p 28

the context. As mentioned earlier, complex interdependence mainly serves to elucidate the economic character of why states cooperate.

Complex Interdependence in the Information Revolution

This conceptualisation of complex interdependence has been updated by Keohane and Nye to reflect the environment of the information revolution and its impact on the international system. The revised version of this theory offers thus offers conceptual linkages between the increased channels of communication in complex interdependence and the introduction of ICT technologies in the information revolution.[146] This is demonstrated by how these communication technologies work as a form of transnational flows that can be accessed by virtually anyone from individuals to what the authors refer to as "loosely structured networks."[147]

The result of this, is that non-state actors such as NGOs and individual actors are now capable of permeating the borders of states, and through communication with their local constituencies, also capable of forcing political leaders to focus on agendas relevant to these non-state actors. The implication of this is changes to the one dimension of complex interdependence that dictates the available channels of communication between societies.[148] This factor is especially pertinent to the discussion on CS cooperation. As pointed out in the EUCSS, a plethora of non-state actors participate in the institutionalisation of CS, thereby reflecting the environment of loosely structured networks. From this perspective, these factors play a significant role in the decisions taken by institutions and state actors, and possibly may have an effect on the relationship between MS and the supranational coordination of CS, as both would be affected by non-state actors to a certain extent.

The crucial change in relation to the impact of the information revolution, however, lies in the cheaper access to communication technologies, thus providing the aforementioned actors and anyone with readily available access to these technologies, the power to carry out communication through cyberspace as a form of transnational flow, according to Keohane and

[146] Keohane, Robert O., and Joseph S. Nye. "Power and Interdependence in the Information Age." Foreign Affairs 77, no. 5 (1998): 81-94. Accessed April 20, 2017. doi:10.2307/20049052., p 83
[147] Ibid
[148] Ibid, p 84

Nye[149] It is important to note that there are different types of information that can be circulated in cyberspace. However, commercial information is outside the focus of this analysis.[150]

Free information is a type of information which is sent by an actor with no intention of a monetary return. On the other hand, it relies on the recipient being receptive to the information passed to them, thus fulfilling the goal of the sender, whether it is in the form of a political message, marketing, propaganda, or anything that may influence the recipient in some form or another. This kind of information is particularly prevalent in the information revolution, as suggested by the cheapened access to communication technologies and its little to no cost.[151]

Strategic information refers to an asymmetrical type of information in that it is advantageous to the actor possessing certain information that its competitor or rival does not possess. As mentioned, it is often seen in the form of military intelligence. It can be argued that this information can also relate to cyber defence capabilities of a state, provided it confers an advantage to the actor possessing this information.[152]

These types of information can also serve contextual purposes for how states evaluate information sharing in the EUCSS through the NIS-Directive, and whether particular types of information serve as a factor for obstacles to information sharing.

As the theory of complex interdependence points out areas where realism maintains a degree of relevance in the areas of security and military issues,and seeing as it is not ruled out as an option despite being unlikely unless the conditions of complex interdependence should fail.[153] It would therefore benefit the analysis to provide a realist perspective of the information revolution. Following the pragmatic approach to IR theory, this will help analyse some of the security issues embedded in CS, and furthermore highlight the limitations of the liberal approach, which primarily concerns itself with the economic aspect of CS.

This is also taken into account due to the increasing reliance on information systems in these domains, and furthermore the importance of these systems for states with access to cyber capabilities in the form of cyber defence,[154].

---

[149] Ibid
[150] Ibid, p 85
[151] Ibid, pp 83-84
[152] Ibid
[153] Ibid, p 84
[154] Ibid, 88

The relevance of Realism in CS

With the inclusion of complex interdependence as an element of the information revolution, thereby bringing its concepts into the CS debate. In this connection, the theory has also argued which areas of the state are still relevant in the information revolution, and thus an important consideration for the topic of CS.

Grieco divides realism into five propositions, where the first point is that state actors are seen as occupying the primary role in world affairs.[155] This is in stark contrast to liberal IR theory which puts emphasis on the role of non-state actors, as mentioned before. Secondly, states are viewed as abiding by the rules of "sensitive to costs"[156] - meaning that states carefully approach situations in international affairs from a rational standpoint due to the costs that may occur. Therefore, they also act rationally.[157] The third point positions international anarchy as the primary determinant for the motives and actions of states.[158] The fourth point refers to how states operating in the international system of anarchy are also driven by power and security. In relation to this, they are liable to conflict and competition, which creates obstacles for cooperation between states. The final point dismisses the influence of international institutions in cooperation initiatives. [159]

The traditional approach to national security, however, can be approached from the realist perspective. Here, states seek their own security with disregard of the security of other states. This connects to the notion that while states cannot achieve permanent peace, they can attempt to balance the power of other states, thus preventing other states from achieving hegemony.[160]

---

[155] David A. Baldwin, *Neorealism and Neoliberalism: The Contemporary Debate* (New York: 1993), p 118
[156] Ibid
[157] Ibid
[158] Ibid, pp 118-119
[159] Ibid, p 119
[160] [160] John Baylis, Steve Smith, and Patricia Owens, *The Globalization of World Politics: An introduction to international relations*(Oxford:Oxford University Press, 2011)., p 234

These classical realist positions on national security can also be reflected in the arguments laid out by the neorealists such as Waltz and Mearsheimer.[161] Here, the international system itself is viewed as a system of anarchy. That is, without a central authority to keep states in check or capable of controlling their behaviour.[162] This ties into the assumption that states develop military capabilities to defend their sovereignty, but also to increase their power. The consequence of this is that now the international system is ruled by anarchy and a lack of trust, states find it difficult to trust one another, thus justifying these capabilities.

Furthermore, survival becomes the top priority and determinant for state behaviour, as states will want to retain their sovereignty and independence in this system.[163] Finally, the true intentions of states are obscured, as they will be incentivised to hide their capabilities. This is where information and obfuscation thereof plays an important factor.[164] These assumptions all tie in to the realist position on national security, from where it is argued that security is dependent on the very structure of the international system, which is inherently anarchic as mentioned earlier. Thus it is also implied that the future of international politics will reflect the violent past, as suggested by some realist scholars such as Mearsheimer.[165]

On the other hand, the neorealist position on cooperation provides insight into the limits to cooperation, as it is argued to be determined by the logic of security competition. Therefore it also restricts the likelihood for a permanent state of peace.[166] Cooperation is also constrained by the concepts of "cheating" and "relative gains."[167] The former concept implies that states constantly worry about other states who might cheat and defect from agreements, and might do so with military power. Therefore the state is constantly worried about this factor and aware of its self-reliance when it comes to matters of national security.[168]

The latter concept of relative gains can also lead to barriers for cooperation, because the concept suggests that states are concerned with their gains in relation to other states in a cooperative engagement. The concept ties back to the idea that states want to maximise their own gains in an

[161] Ibid
[162] Ibid, p 235
[163] Ibid
[164] Ibid
[165] Ibid
[166] Ibid
[167] Ibid
[168] Ibid, p 236

international system that is anarchic and therefore uncertain.[169] This ultimately leads to an environment of distrust, thereby complicating the options for cooperation.[170]

This provides a cursory look of an IR realist perspective. While it may give an idea of how a state would approach the complex issues of cooperation and conflict in CS, it does not communicate directly with the information revolution literature, and thus the debates around the impact of information technologies in international politics.. The following section will address this point.

Bridging the gap between Realism and the CS literature

Currently, realism has approached the information revolution and CS literature from the perspective of military capabilities. That is, the introduction of ICT technologies in world affairs is seen primarily as an extension of state military capabilities, thus also arguing for the limited role of non-state actors in this domain. Here, it is seen as a continuation of the information warfare dimension of the military, along with other aspects of electronic warfare. Thus it is argued that it follows the military logic of defending and attacking information and its systems, according to the realist perspective. [171]

Although the realist view recognises that information security may play a role domestically and politically for a state, it is argued that it does not affect the anarchic international system in any shape or form.[172] Instead, information/CS is viewed from the perspective of an economic issue which dismisses security threats from cyberspace and thus of no challenge to the state as the primary unit in this system of anarchy.[173]

Based on the realist interpretation of the information revolution and CS as an extended concept, it becomes apparent that there exists a gap between liberal and realist interpretations of CS and how they approach cooperation and conflict within this field. On the other hand, it can also be argued that both theoretical approaches offer complementary explanations of CS from the pragmatic approach to IR theory.

---

[169] Ibid
[170] Ibid
[171] Johan Eriksson and Giampiero Giacomello, *International relations and security in the digital age*, p 229
[172] Ibid
[173] Ibid

While the liberal interpretation of CS reflects the multitude of institutions and non-state actors involved in political CS frameworks, it also focuses on primarily the positive aspects of the inclusion of information technology, including why states choose to engage in institutional cooperation initiatives as a positive venture.[174] Furthermore, with its focus on non-state actors and their transnational capacities, it also puts economic matters on the same level as security.[175] In doing so, it also assumes that institution building and international norms can overcome conflicts. In connection with this, collective and cooperative types of security have also been promoted, while also doing away with realist conceptualisations of security.[176] Moreover, liberalism has also assumed modernisation and technological development to be purely a positive development.[177]

The realist approach can be applied to analyse this theoretical gap left uncovered by liberal IR and thus the liberal institutionalist approach. The purpose of this is to elucidate parts of the analysis, wherein it is argued that the liberal perspective falls short of explaining why states take certain actions within CS cooperation engagements that fall outside the logic of the liberal institutionalist theory. Despite previous criticisms that realism narrowly defines IT-threats as economic issues[178], there are empirical cases where realism can be linked to security perceptions of CS. For instance, The United States officially regards cyber space as the "fifth domain" in warfare. In addition, NATO considers cyber conflict as a threat to its collective security clause.[179]

With this is in mind, it is also worth to consider the previously mentioned goal of the EU to align the framework of the EUCSS with that of the NATO and US approaches to CS security. There is then arguably empirical evidence for a realist consideration to CS engagements, and what implications this has for cooperation and conflict in CS.

One way to theorise about realism in CS is by utilising Tuthill's application of Waltzian structural realism in the analysis of the digital world.[180] In his thesis, Tuthill seeks to carry over

[174] Ibid, p 230
[175] Ibid
[176] Ibid
[177] Ibid
[178] Ibid, p 229
[179] Friis, Karsten, and Jens Ringsmose. *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*. ,p 65
[180] David Paul Tuthill, "Reimagining waltz in a digital world: Neorealism in the analysis of cyber security threats and policy," Ph.D. dissertation, University of Kent, March 2012., p 12

Waltzian tenets of realism to the cyber debate.[181] This is carried out through the following conceptualisations: First of all, Waltz envisions systems as the main reasons for why actors seek power.[182]

The system itself is static, but it defines clear rules of behaviour that dictate survival. Therefore it is up to the actors to act according to its rules, if they wish to survive within this system. The system itself is evidenced by disconnection between actions and outcomes in the international sphere.[183] In relation to cyber, the Waltzian theory has been applied to networked systems, which posit that the international system is a network that consists of objects in the form of states[184]

Anarchy forms the basis for the entire system of international relations and dictates the self-help system embedded in realism. Anarchy in the internet can be seen as decentralised architecture that has gone from simply a military communications tool to a global communications infrastructure used by public and private sectors alike.[185]

Power is realised in the anarchic system. The units therein, or states are similar, apart from the capabilities they possess. Power from the Waltzian perspective is then the only variable in the international system, and also the only available option for states to improve their power. The way this is done is through states increasing their power relative to other states in this system. This is also known as relative gains. That is, power must come at the expense of power from another actor.[186]

Following this, it is noted that Waltz from a defensive realist perspective sees a transition in the state as a power-seeking unit, to a security-seeking unit. Namely that maintenance of security is now the main concern of the state. Thus, the primary concepts in international politics are both "security, stability, and preservation of the status quo" rather than aggression. This defines the defensive type of realism.[187] In the cyber debate, this can be envisioned as the intangibility of power in cyberspace. Tuthill thus relates this to the idea maintaining autonomy as

[181] Ibid
[182] Ibid
[183] Ibid
[184] Ibid
[185] Ibid, pp 12-13
[186] Ibid, p 14
[187] Ibid

the central idea of power.[188] This is then contrasted with cyberspace, where the distribution of power is argued to be high due to the fact that both nation states and non-state actors (organisations) seek security in some shape or form. Similarly, some non-state actors want money, others attention, and others knowledge. These concepts can all materialise as power in cyberspace.[189]

The idea of fundamental distrust and the problem of attribution can also be related to the CS debate. The basic idea is that an environment of distrust is established because states can never know the true intentions of other states. Furthermore, states are left to their own devices through the self-help principle in realism, and therefore they cannot rely on help. Thus, in alliances with state at relative levels of strength, defection of a state can jeopardise the security of the remaining states. Tuthill then connects these concepts with Mearsheimer's notion that states always seek to increase their relative power to alleviate this problem.[190]

CS faces a similar problem as attribution is difficult in this decentralised structure, but this also creates distrust among states, it is argued.[191] One of the reasons for this is the difficulty of attribution in cyber attacks.[192]Thus, it is possible to draw connections from these concepts of structural realism to the CS debate, and furthermore, apply them in the operationalised framework.

Theoretical foundation of Cyber and Security

Having covered the traditional IR assumptions about security, it is then possible to move on to how security is conceptualised in the information revolution debate as CS, and at the end of this section, linkages can be drawn between both literatures, but also what will be argued to be the recontextualisation of security in CS. This theorisation is thus created to establish the security perspective which will be used to relate to the CS debate in the EUCSS.

[188] Ibid, p 15
[189] Ibid, p 15
[190] Ibid
[191] Ibid
[192] Ibid, pp 15-16

One salient way to conceptualise cyberspace is through a common definition of "all computer systems and networks in existence, including air-gapped systems."[193] This definition provides a foundation for the systems included in cyberspace. A further elaboration of this concept also includes the internet itself as it covers all computers connected to its domain, as well as the world wide wide web. The final aspect refers to a so-called "cyber archipelago"[194] which consists of all the computer systems not directly connected to the internet, but still pose significant security considerations.[195] These exist in the form of critical infrastructures such as power plants and other systems that provide necessary services to societies, whether in the form of water, electricity or heating.

CS as a concept can also be approached in multiple ways, highlighted by the fact that the term "information security" encompasses related aspects of CS such as protection of information flow in society, related to regulation of censorship on the internet.[196] For this reason, it is deemed crucial to delimit this concept with respect to the analysis in this thesis.
Kello provides a definition of CS that describes the phenomenon as consisting of "measures to protect the operations of a computer system or the integrity of its data from hostile action."[197]

Upon further elaboration, it can also include a particular state of affairs. This would be any absence of intrusion into a computer network or system. This rests upon the idea that CS is preventing unauthorised access to take place in relation to these networks.[198] Moreover, it can also be conceptualised as "information security" which directly involves government protection of information flow channels in society.[199]

The definition given by Cavelty expands on this notion, and provides some additional insight into the topic being studied in this thesis. Here CS is referred to through a broader term of "information age security", which essentially consists of two categories. One being defensive activities, meaning information assurance, also known as critical information infrastructure protection (CIIP). The other is offensive activities, referring to the concepts of information

---

[193] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013): , accessed April 20, 2017, doi:10.1162/isec_a_00138., p 17
[194] Ibid
[195] Ibid, pp 17-18
[196] Ibid, p 18
[197] Ibid
[198] Ibid
[199] Ibid

warfare, cyber terrorism, and cyber-crime.[200] Cavelty notes that these issues are all tied to the information revolution, cyberspace, and the overall information infrastructure.[201] Therefore, it can be argued that the CS debate is tied to these notions, as it covers all the ongoing activities within this dimension.

An important distinction made in this regard, is how information age security consists of both physical components in the form of broadband networks and satellites, but it is consists of a virtual or cyber component in the form of the information being passed through networks and the overall information infrastructure. This also includes the knowledge and services created in cyberspace.[202]

Thus, Cavelty notes that security in this context connects to both virtual and physical dimensions. In this connection, it is also concerned with threats from the information infrastructure, but also threats against it. In this regard, cyber threats are defined as a non-specified force, apart from its malicious use of information/communication technologies[203]

It can be argued that these factors contrast the previous understandings of security, as these systems provide an additional challenge to states and institutions, in the form of information systems that are often controlled by these non-state actors and organisations. Furthermore, the information revolution is characterised by a multitude of communication and information technologies that essentially function as a global and decentralised network of communications.[204] Therefore these networks also challenge aspects of the traditional notions of security from the IR paradigms, such as territorial borders, and the blurring of civilian, political, and military boundaries, thereby leading to a significant distribution of power in societies.[205] As an extension of these developments,

Cavelty points out two schools of thought in the cyber literature. One is driven by cyber-enthusiasts who emphasise that these technologies empower societal actors, and can establish

[200] Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia. Krishna-Hensel, *Power and security in the information age investigating the role of the state in cyberspace,* p 22
[201] Ibid
[202] Ibid
[203] Ibid
[204] Ibid,p *2*
[205] Ibid, pp 4-5

cooperation between state and non-state actors, and can thereby have a democratising effect on society.[206]

However, the cyber-pessimists see these technologies as carrying risks, such as threatening identity, and could leave society vulnerable to various forces of control. Risks to infrastructures and the presence of malicious actors are taken into account here.[207]

In sum, these theoretical perspectives on CS can be reflected in the IR liberal and realist applications on European CS, and thus provide counter-points to the IR theoretical perspective, and show how these IR assumptions about cooperation and conflict must be contextualised in the greater context of CS.

Defining Power in Cyberspace through the concept of Cyber Power

Cyber power is included as a tool of power in the CS debate, in order to show the means of power available to actors in cyberspace. In this regard, it serves an important explanatory purpose for what actions and policy tools are available to actors in cyberspace. While the three major conceptualisations of cyber power have been discussed in the literature, it is in the interest of the thesis to apply one of these notions, as both Nye's and Betz and Stevens' conceptualisations share similarities in their explanations of what cyber power entails and how it is utilised by actors. In this regard, Betz and Stevens argue that cyberpower is the "manifestation of power in cyberspace rather than a new or different form of power."[208]

The approach to cyber power outlined by Betz and Stevens present four dimensions of basic power in which cyber power operates. However, it is outside of the scope of the thesis to consider productive cyber power, as it mostly focuses on discursive acts of cyber power.[209] Therefore the following three types of cyber power will be considered:

[206] Ibid, p 5
[207] Ibid, pp 6-7
[208] David J. Betz and Tim Stevens, "Power and cyberspace," *Cyberspace and the state* 51, no. 424 (November 30, 2011): , accessed February 18, 2017, doi:http://dx.doi.org/10.1080/19445571.2011.636954., p 44
[209] Ibid, p 50

Compulsory Cyber Power

The first of these is compulsory cyber power. This can effectively be described as the ability for an actor in cyberspace to utilise coercion, and thus the ability to change behaviour and certain conditions for existence for other actors in cyberspace.[210] Thus, the aim of coercive action is for one actor to seize control of a network system or computer systems and control its behaviour, in order to modify the behaviour of another actor.[211]This type of coercion can be utilised by both state-actors and non-state actors alike.[212]

In essence, there exists a plethora of actors in cyberspace, and the only requirement for an actor to participate in compulsory cyber power is access to cyberspace and technological know-how.[213]

Institutional Cyber Power

The way in which institutional cyber power is typically carried out, is when one actor seeks to influence or even limit certain actions of another cyberspace actor through the use of several types of institutions. This includes media institutions to influence opinions on certain issues, domestically and transnationally, as well as and state-sponsored institutions who are capable of setting particular norms and standards within cyberspace, which can then also influence and decide the actions available to another actor in cyberspace.[214]

An important element of this type of cyber power is that it can take place through several types of intermediary institutions, working at both the state level[215], but also at the sub-state level through institutions tasked with setting a certain working culture or approaches to CS related issues, which are in line with the overall national CS strategy[216] This practice is often

[210] Ibid, p 45
[211] Ibid, p 46
[212] Ibid, p 45
[213] Ibid
[214] Ibid, p 47
[215] Ibid
[216] Ibid, p 48

coordinated by the state, but is carried out by intermediary institutions that reflect the CS practices and goals of the state, effectively seeking to instill a certain type of behaviour in both non-state professionals and employees under the government.[217]

Structural Cyber Power

Structural cyber power is concerned with maintaining the structures in which cyberspace actors are located, and thus also determine the actions available to these actors. Contrary to both the institutional and compulsory cyber powers, this type deals with how cyberspace itself creates certain structures which cyberspace actors must then adhere to. Therefore, it is about the internal structures, rather than external actors exerting cyber power.[218]

There are different ways in which this phenomenon has been approached in scholarship and linked to structural cyber power. Here it is noted by various scholars as the: "transition of industrial economies to post-industrial ones based on the commodification of data, information, and knowledge."[219] Rather than asserting that the information technologies have had a transformative effect on social organisation in society, it is argued that the structural power that has been present since the industrial age is still manifested in the network society, including the structural positions of capital and labor.[220]

[217] Ibid
[218] Ibid
[219] Ibid, p 49
[220] Ibid

Conceptual Framework: A pragmatic approach to cooperation and conflict in the European Cyber Security Strategy

The following framework builds on the previously mentioned theories together with considerations to the theories, which seeks to draw them into the context of CS and therefore build an approach that can be operationalised in the analysis. First of all, this focuses on how the EUCSS attempts to construct a collective idea of CS involved in the cooperative engagement with the selected MS. Secondly, it then focuses on how MS construct their idea of CS through their national strategies. Using a pragmatic approach, focusing on liberalism and realism, it will then be analysed how these theories explain these approaches to CS, and identify areas within the national strategies, where they highlight cooperation with the EU on CS, and where these strategies conflict with the overall EUCSS and NIS-Directive. Through this analysis, the context of CS is also analysed in relation to these IR concepts. That is, some areas of cooperation may involve both realist and liberalist approaches to CS, whereas other areas might reference a realist state-centric approach, and therefore this falls into the conflict dimension, as it contradicts the EUCSS notion of collective CS. This is also the dimension, where states may use an alternative third approach, of cyber power, as a form of soft power in CS engagement. Finally, it will be possible to point out areas where CS is contextual, and thus also show the limits to these IR theoretical perspectives when analysing the phenomenon of CS. The contextual analysis will be taken into account in the cooperation and conflict dimensions.

Thus, it will be possible to draw up the liberal and realist IR perspectives involved in the two dimensions, which also serves as the conceptual framework:

Cooperation Dimension

First of all, the cooperation dimension builds on the liberal institutionalist approach, based on the principles covered in the theory. That is, it sees cooperation through institutions as providing the state with several benefits, which this includes ensuring absolute gains, facilitating benefits for interaction between states, and a stable environment of cooperation between states. Furthermore, institutions prevent cheating in agreements, ensuring that states are locked into commitments and do not defect from institutions.

In sum, the liberal institutionalist perspective on cooperation rests on the notion that cooperation provides a variety of benefits to states, as well as ensuring that states stick to their engagements in institutions. Moreover, complex interdependence can be seen as part of this cooperation dimension through how it allows multiple channels of contact between actors, both domestic and transnational. Cooperation can thus be achieved through increased interaction between both state and non-state actors, which in turn can also increase cooperation between these entities. Cooperation between states and organisations or private companies is one such example. This is also reflected in the institutional set-up of the EUCSS, where cooperation in the form of public-private-partnerships and dialogue with civil society on cyber issues is directly encouraged.[221] This is also materialised in the transnational and transgovernmental condition of complex interdependence. The blurred line between what can be classified as domestic or international politics is especially relevant in regards to the EUCSS, as the interaction is affected by transnational relations.

Moreover, this raises the point of contact between governmental bureaucracies which, according to complex interdependence, can have the power to change the perceptions of national interests, if the interests of the agency are pursued as national interests. This also raises an important point that must be considered for the analysis of cooperation under the EUCSS, as each national CS strategy is involved with their national bureaucracies to some extent. In addition, the liberal institutionalist perspective places institutions as the central tenet of cooperation in this dimension. As a consequence of this, the cooperation aspect will primarily focus on the role of the EU as an institution that coordinates the EUCSS and the NIS-Directive.

However, it can also be argued that structural realism and cyber power can explain aspects of cooperation in CS. While both liberal institutionalism and structural realism recognise the role of the state to different extents, structural realism sees the state as the central unit of power in this regard, but also capable of engaging in institutions for if it carries over benefits for the state apparatus. While it is recognised that both theories include the state as a dimension of international politics, the focus with the realist perspective will deal with the state as the focal point of CS cooperation. In addition, cyber power displays the array of tools available to actors

[221] Appendix 1, p 12

in cyber space, for instance including the ability to influence institutions to obtain objectives in cyberspace.

Conflict Dimension

The conflict dimension is reflected in the realist theoretical perspective through its reference to the realist positions of the concept of power, which assumes that states are egoistic actors, driven by their own self-interests. From this position, it can be argued that CS would be problematised by the interests of states in cyberspace, such as safeguarding information and developing cyber undisclosed cyber capabilities.

The report from the ENISA Agency that some states were reluctant about sharing CS information across the EU grants credence to this assertion. One realist assertion that has been noted earlier is that the distribution of power in cyberspace is relatively high, when it follows the notion of power as maintaining autonomy. Therefore it is not always clear how a state would pursue its own state interests in cyberspace, as power is distributed among several different key actors, such as private organisations who are in control of many of the CS related systems.

Cyber power can also be used by actors to achieve certain gains in cyberspace over the expense of others. Furthermore, it can be argued that it becomes difficult to attribute offensive actions taken by actors in cyberspace, if the realist assumption about lack of attribution rings true. Asymmetrical capabilities and strategic goals can also be a factor from this perspective, which would be problematic for a strategy that intends to harmonise a coordinated response to CS.

Sub-conclusion: Theory

The theoretical perspectives presented here highlight the complexities in the application of the IR theory brought into the CS debate. As a result, the respective theories each provide explanations as to how cooperation and conflict take place in the domain of CS. However, it can also be argued that liberal institutionalism is better suited to explain the environment of CS, as it reflects the variety of transnational actors and non-state actors, each providing their own input to institutions in CS. This is followed by the recognition that certain aspects of these societies are outside the full control of the state apparatus, e.g. critical infrastructures. Although, this is also followed by the caveat that liberal institutionalism may leave certain aspects of CS cooperation unproblematic, while also taking certain considerations for security for granted.

The structural realist and cyber power perspectives provide possible explanations as to why cyberspace presents a unique issue to states through its borderless nature in many aspects. Hence, why a fundamental lack of attribution and anarchy may lead states to attempt to secure parts of cyberspace, and in some cases, establish borders through either attempts to control flows of information and limit access for certain actors. This also includes states furthering their own interests through cyber power, in order to secure their positions in cyberspace. This also serves as the counterpoint to complex interdependence, which is characterised by loosely structured networks and transnational flows of communication. The structural realist position in the CS literature would arguably attempt to curb these actions. Thus, this sub-conclusion can be listed as such in relation to the cooperation and conflict dimensions:

Pragmatic IR theoretical approach	Cooperation	Conflict
Liberal Institutionalism	- Institutions as beneficial to cooperation - Institutions provide information on agreements - Complex Interdependence increases channels of contact between state and non-state actors	- Assumption that modernisation is inherently good - Economic perspective takes security issues for granted - Complex interdependence may take malicious non-state actors for granted
Structural Realism	- Institutions beneficial if they serve state interests - States become security-seeking units	- Lack of attribution in cyberspace - Cyberspace exists in a system of anarchy - Intangibility of power
Cyber Power	- Cyber power as a means to further domestic interests in the international sphere - Can set structural rules for CS cooperation	- Asymmetric cyber power capacities between actors in institutions - Structural cyber power limit options available to actors
Cyber Security Literature	- Cyber enthusiasts see democraticisng effect of CS - Increases interaction between societal actors - Empower actors	- Information can become hostage to certain actors and vulnerable - Risks to infrastructures - Malicious actors with unknown intentions

Analysis of European Cyber Security

Analysis of the European Cyber Security Strategy and the NIS-Directive

The EUCSS presents itself as a cooperative engagement working through a multitude of public-private-partnerships, working groups and the ENISA Agency, in order to establish a coherent CS strategy on an EU level, taking both public and private factors of CS into account.[222] The strategy presents three primary objectives as the driving force behind the strategy.

One of the first observations in the strategy pertains to the presentation of European values as being ultimately tied to the notion of an "open and free" cyberspace.[223] This objective describes the ideational aspects of the CS strategy that connect the offline values of the EU to online values enshrined in the EUCSS, including democracy, rule of law, and fundamental rights.[224]

In the second objective, the plan suggests that this type of virtual freedom requires safety and security, similar to the physical world.[225] In order for this to be realised, the plan suggests a multistakeholder approach. First of all, it is suggested that the private sector as well as civil society must be the main driver of growth for this to succeed. The private sector is also seen as a crucial part for security to function online, as most of cyberspace is run by private companies. Thus, the initial assessment of the private sector involvement implies a particular liberal market rationale for CS. The plan also emphasises the regulatory aspects of governments as particularly

[222] Appendix 1., p 2
[223] Ibid
[224] Ibid
[225] Ibid

important in terms of regulation. They have the roles of securing access and the function of the internet.[226]

Following this, it becomes apparent that the strategy is underpinned by a liberal approach to CS, where the internet is required to be both robust and innovative, in order to secure freedom and prosperity.[227] Thus in order it secure the ideational aspect of EU values in cyberspace, the private sector and civil society are seen as vital to this process. This reinforces the liberal institutionalist approach taken within the framework of the EUCCS, and it also describes the blurred lines between the role of the state and private sector, specifically in relation to their respective capabilities and responsibilities. In addition, the dynamic relationship between the private sector and governments described in the EUCSS strategy, follows the information revolution literature that describes the natural progression toward a multistakeholder approach in liberal societies, where the private sector and information structures are owned by ICT companies and owners of critical infrastructures.

However, the liberal institutionalist assumptions are also left unproblematic in this part of the strategy, as it rests on a form of security tied to economic interests. One criticism that can be aimed at this approach is the seemingly positive assumption about the economic values in cyberspace. On the other hand, one can also argue that this is contextual to the CS literature, where the enthusiastic side of the CS debate takes certain security matters for granted, while encouraging interaction between actors. This is arguably an area where liberal institutionalist assumptions

Furthermore, It can be argued that the cooperative mechanism driving this strategy is driven by a liberal institutionalist logic in how it presents engagement with MS on CS issues. This factor is present in how the strategy directly encourages cooperation between these MS, based on the embedded promise that states will achieve absolute gains through this engagement through the institutionalised reciprocity present in the EU institution. The reciprocity in this case, is the information exchange that takes place in this cooperative engagement. Therefore the EUCSS also rests on the promise that if the MS cooperate within the agreed parameters, such as

[226] Ibid
[227] Ibid

safeguarding the functional aspects of the internet, they will also secure the economic system of the EU, in the form of the Digital Single Market.[228]

The third objective relates to the economic aspect of the strategy. Here it connects the ICT technologies and thus the cyberspace dimension and compares it to the "backbone of our economic growth."[229] This point further highlights a liberal approach to CS, where the the idea of security in cyberspace becomes connected to economic aspects of liberalism. It also points to certain aspects of liberalism in the information revolution literature. Here it is present in the form of fragmented monopoly on authority through transnational non-state actor networks. In the EUCSS, this is demonstrated by the presence of civil society and private actors engaging in the institutionalisation of CS.[230]

It is important to note that the underlying commercial logic behind this part of the strategy, in the Directive, is based on the legal provisions pertaining to the internal market of the EU and its functions. Simon and de Goede have noted how this is explained as: "the logic of market integration becomes written into the security code here, while simultaneously the security logic of protecting infrastructures becomes part of market rationale."[231] This perspective thus builds on a liberal institutionalist notion that high and low politics become interrelated, as seen here in the diffusion between security and economic provisions.

It also illuminates the approach taken to CS in the strategy, as it also shows some tensions between traditional approaches to security and governance, where in this case, CS is a mosaic involving private companies, nation states, and institutions.[232] This also reflects the larger rule-set of internet governance which involves several different interest groups, each with their own policies in the aforementioned groups.[233]

---

[228] Ibid
[229] Ibid
[230] Ibid
[231] Simon, Stephanie, and Marieke De Goede. "Cybersecurity, Bureaucratic Vitalism and European Emergency." *Theory, Culture & Society* 32, no. 2 (January 14, 2015): 79-106. Accessed February 4, 2017. doi:10.1177/0263276414560415., p 95
[232] Laura Denardis, "Hidden Levers Of Internet Control," *Information, Communication & Society* 15, no. 5 (February 16, 2012): , accessed May 5, 2017, doi:10.1080/1369118x.2012.659199., p 722
[233] Ibid

An important factor to consider in this form of internet governance, is the presence of technical arrangements, where political values are embedded in these internet governance technologies.[234] While institutions have and do play a significant role in establishing public policies in CS, the technical architecture is in itself an arrangement of power and not removed from political influence.[235]

Furthermore these architectures for instance exist in the form of domain names, IP addresses, and critical internet resources. One example where this political tension is present is through internet protocols.[236] Besides having a technical function, such as providing accessibility to the web, these protocols are also underpinned by certain political and economic values. One mentioned example by DeNardis is encryption standards which must balance individual privacy and national security concerns, as well as functions for law enforcement.[237] In addition, these economic and political interests often take place through companies or private standard-setting institutions.[238]

All of this architecture is influenced by political and economic values through its administration and design.[239] On one hand, the architecture behind the internet is one additional layer to the fragmented monopoly on authority in cyberspace. The internet governance responsible for technical design decisions and legal matters behind the architecture is not constructed purely through economic interests. Rather, there are also political interests and values of groups that must be taken into account in its construction.[240] In relation to the EUCSS, it becomes apparent that the fragmented monopoly on authorities is present throughout political interests from state actors, civil society, and then also groups behind specific technical processes related to the function and maintenance of the internet.[241]

An additional layer to this analysis can be found through the application of cyber power. From this perspective, it can be argued that the architecture behind the internet, and thus intrinsically tied to CS is governed through a form of structural cyber power. That is, how the

[234] Ibid, p 721
[235] Ibid
[236] Ibid, p 723
[237] Ibid
[238] Ibid
[239] Ibid
[240] Ibid, p 722
[241] Ibid

internet itself establishes structures that actors must face and adhere to its principles. In this regard, the structural power present since this industrial age is replicated in cyberspace, as evidenced by the technical architecture of the internet that contains underlying economic and political influences as a form of structural cyber power. This type of cyber power is arguably something both the EU as an institution must face, but also the states involved in the EUCSS and NIS-Directive, as well as other actors. This is specifically due to the structure of this cyberspace, as it serves fundamental functions which the CS strategies are based on.

Therefore it also reflects a wide variety of interests in this type of governance, as opposed to traditional nation state governance, with a particular area of jurisdiction.[242] This tension is also observed in the case of ENISA, which also serves to coordinate between MS on areas of CS coordination. ENISA, on the other hand, is considered to be removed from political accountability, as it presents itself as being outside the domain of politics. The same applies to Europol.[243]

As a result, the EUCSS framework is on one hand delegating coordination responsibilities to these apolitical actors such as ENISA and CERTs in the NIS-Directive,[244] but on the other hand, these actors are coordinating CS strategies that rest on a specific form of structural cyber power in relation to the architecture of the internet. Moreover, it can be argued that these apolitical actors will have to coordinate through a form of institutional cyber power, reflected in the European strategy itself. Thus, from the cyber power perspective, this is present through the institutional norms and standards set by the EUCSS. When this factor is taken into account, it becomes evident that the EUCSS itself already operates through two layers of cyber power. While the ENISA agency is officially listed as an apolitical entity in this CS engagement, there are still some concerns with how this is reflected in the coordination of the strategy as pointed out here.

Therefore, there are concerns about how ENISA avoids political accountability in this regard.[245] Yet, the inclusion of cyber power helps shed light on how agencies such as ENISA are

[242] Ibid
[243] Simon, Stephanie, and Marieke De Goede. "Cybersecurity, Bureaucratic Vitalism and European Emergency.", p 95
[244] Ibid
[245] Ibid

still affected by the political motivations of the institutions they engage with, and therefore cannot remain entirely apolitical in the case of the EUCSS.

Moreover, it can be argued that there is a third layer of cyber power, in the form of the state actors who are then faced with structural cyber power in the form of the rule-sets surrounding the internet, but also the cyber power present in the intermediary institutions through institutional cyber power. These types of cyber power thus highlight the complex relationships between state actors and institutions, as well as the underlying regulations and norms behind the internet architecture. This factor also becomes an important consideration when analysing the individual cases of national CS strategies later, as it will be possible to analyse the use of cyber power from the state perspective, but also in relation to the liberal institutionalist notions about the EUCSS, and how cyber power fits into this part of the analysis. Furthermore, it may explain obstacles to establishing collective cyber security in the EUCSS due to underlying interests in cyberspace itself, which the strategy and Directive will have to coordinate around.

In merging these two theoretical perspectives, it is possible to add an alternative perspective to the aforementioned relationship dynamic in the EUCSS, in which the primary tension relates to these layers of cyber power with liberal institutionalism. This also challenges aspects of the liberal institutionalist focus that are left unproblematic in this debate about CS cooperation, such as the idea that all political issues are granted an equal amount of attention in institutions.

The liberal institutionalist perspective is thus present in the assumption that actors outside the state apparatus are essential to what the EU deems to be a functional CS strategy. For instance, in the document released by the European Commission, the private sector is ascribed a pivotal role in the CS strategy, which follows the liberal institutionalist and complex interdependence assertions that multiple channels of contact provide an environment of interaction between actors. Furthermore, this ascribes a liberal institutionalist approach to governance, which rests on the notion that the linkages created by institutions, ensure that the interests of all actors are given equal weight. However, one can also argue that this also serves as a diffusion of power in relation to CS, as it becomes unclear where the power rests in certain situations, including the traditional security role of the state from a realist perspective.

This is also reflected in the aim of the EU strategy, where the principles of CS specifically address the internet as the "borderless and multi-layered internet."[246], and furthermore asserts that it has become "one of the most powerful instruments for global progress without governmental oversight or regulation."[247]From the IR perspective, this creates the assumption that the internet, as envisioned by the EU strategy, is not defined by the traditional notions of sovereignty with clearly defined borders, as the realist perspective would assert. In addition, it clearly defines the cyber domain/internet as an entity out of reach for governments, with limited competences of regulation.

Furthermore, this is defined by the assertion that governments have limited capabilities in this domain, as well as no state authority in terms of regulation or oversight. Additionally, this gives credence to the liberal institutionalist perspective which then suggests that the only option to achieve control in this domain, is through institutionalisation of the internet/cyberspace, and thereby achieve regulation and oversight as part of a CS strategy. It can be argued that this represents the blurred lines of responsibilities in CS, where responsibilities and capacities become blurred due to this multistakeholder approach, and the fact that private companies operate many of the critical infrastructure systems and information services. One caveat to this perspective, is the notion that the lack of state control in this area is assumed to be unproblematic, as long as CS is institutionalised. However, the EU strategy does also formally recognise this approach to CS and outright states that it is a "shared responsibility to ensure security."[248] In this provision, the strategy also calls for all actors to protect themselves, but also be able to deliver a coordinated response, with the purpose of strengthening CS.[249]

However, some issues have been raised pertaining to the ability of for instance MS to carry out coordinated responses as part of the NIS-Directive, which also calls for information sharing in this regard.[250] This has previously been highlighted as an obstacle to coordination of CS between MS in an ENISA report from 2015, where it is stated that information sharing is

[246] Appendix 1, p 3
[247] Ibid, p 3
[248] Ibid, p 4
[249] Ibid
[250] Ibid, p 6

problematic between MS as it requires high levels of trust between these members, especially in matters pertaining sovereignty issues or national interests.[251]

One can argue that the states in this situation follow a realist security logic to the issue of information sharing, as it is viewed as an issue that is sensitive to costs. That is, information sharing related to CS capabilities arguably presents itself as a security sensitive issue to states from this perspective, which is taken into consideration when approaching an institutional engagement.

In addition, the issue of fundamental distrust can also be raised in this regard, which posits that states can never know the true intentions of other states or actors in the international system, as it is ruled by anarchy. This principle would thus also apply in the case of institutionalised CS. In this case, the problem highlighted by the ENISA agency points out elements in CS that evidently show areas of distrust among certain MS, supported by the realist approach to cyberspace. From the realist approach to CS, one can also point to the state as a power-seeking unit.

However, in the age of cyberspace, it is argued that the state is now a security-seeking unit. As a consequence of this, security is the primary concern of the state in relation to CS. This may explain states show a reluctance to share information within the EUCSS framework, as it might bring to light the security interests of these states. Although the ENISA report also highlights information sharing capabilities as a factor of this issue, it does also state that national interests prevail, especially in public health related matters, where protection of their own populations is highlighted as the top priority.[252]

From a realist perspective this also highlights the problem areas related to establishing global governance around the issue of CS, as it is merely an enhancement to the traditional tools of power available to the state.[253] This can thus help explain why states approach CS as a security-seeking unit as it becomes a capability in the form of a statecraft tool. The cooperative aspect of CS then becomes an extension of individual interests, where states enter these CS engagements from a relative gains perspective, thus granting them cyber capabilities in the form

[251] "Report on Cyber Crisis Cooperation and Management,", pp 15-17
[252] Ibid, p 17
[253] Miguel Alberto Gomez, "Identifying cyber strategies vis-a-vis cyber power," *2013 World Cyberspace Cooperation Summit IV (WCC4)*, November 2013, , accessed May 5, 2017, doi:10.1109/wcs.2013.7050504., p 2

of CS.[254] The problem areas highlighted by the ENISA report show the information sharing aspect as a security sensitive issue among states, which shows that CS is still a sensitive issue to some states when it concerns information.[255]

This problematisation has also been brought up by Peter Round, director of the European Defence Agency, where he states that the problem of information sharing relates to the fact that several MS conceal information about their development of cyber capabilities. He compares the development of cyber capabilities to the early days of gunpowder, where these states gain a capability, and are then reluctant to share it due to the advantages and leverage it provides over other states. In some cases, this has also become a national and sovereign issue of states.[256] The issue brought up relates back to the problems of information sharing identified by ENISA, and also supports the presence of state powers in CS. Although, the EUCCS itself recognises that it is largely the responsibility of MS to deal with the challenges of CS[257], there also seems to be a contradiction between this part of the EUCSS, and the information sharing facilitation carried out by ENISA.

The problematisation of information sharing also leads to the question of how the EUCSS through the NIS-Directive seeks to establish a mandatory reporting network for CS issues among MS, if these issues are present, especially when taken into account that the issues of information sharing are brought forth by powerful EU MS.Despite this, the strategy does recognise the fact that MS carry the primary task of security challenges in relation to cyberspace.[258]

[254] Ibid
[255] Report on Cyber Crisis Cooperation and Management,", p 17
[256] "Cyber security directive held up in face of 'Wild West' Internet," EURACTIV.com, April 17, 2015, , accessed May 24, 2017, https://www.euractiv.com/section/digital/news/cyber-security-directive-held-up-in-face-of-wild-west-internet/.
[257] Appendix 1, p 4
[258] Appendix 1, p 4

However, it still calls into question how the EU then envisions the strategy as complementary to the state responsibilities of security. In this connection, the EUCSS outlines five strategic priorities that serve to address the performance of the EUCSS. These are listed as:

> "Achieving cyber resilience, drastically reducing cybercrime, developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP), develop the industrial and technological resources for CS, Establish a coherent international cyberspace policy for the European Union and promote core EU values."[259]

While each strategic goal addresses different capacities and aims of the strategy, it also outlines the requirements for MS and similarly what the EU intends to do in order to cooperate with MS on these CS issues. Here the strategy elaborates on how the NIS-Directive component will ensure that these provisions are carried out.[260]The IR perspective on these issue areas will be applied, in order to analyse how the EU seeks to establish a sense of collective security through these principles, and also potential areas where states may object to cooperation on these security matters. Therefore the first point of achieving resilience is pertinent to this analysis as it describes how the EU conceptualises resilience as a type of CS..

One point to make here is the idea of resilience through cooperation and coordination between public and private sectors. This is connected to the market logic to security, which supports the notion of internal security in the EU.[261] This goes back to the assumption that CS is driven by a liberal institutionalist notion of institutions providing security. In this case, it is thus translated to the domain of CS. Additionally, this ties into the NIS-Directive that grants the necessary resources for the public and private sectors to cooperate. In this case, the EU proposes legislation which is supposed to enhance the NIS competencies and set specific requirements for NIS authorities in the different MS.[262]

The objective of the EUCSS to achieve a specific level of CS takes place through this phenomenon of resilience, which rests on the liberal institutionalist notion that cooperation through what the strategy refers to as development of capabilities between the private and public

[259] Appendix 1, p 5
[260] Ibid, p 5
[261] Ibid
[262] Ibid

sector. The use of resilience in this regard thus rests on the liberal institutionalist notion of cooperation taking place through a multitude of state and non-state actors.

This is strengthened by the idea of cyberspace and threats emanating from it are ultimately of a cross-border character. Therefore it requires transnational cooperation to achieve resilience as a form of CS. In addition, the logic behind this resilience is ultimately to secure economic interests, in the form of maintaining the function of the internal market. However, there are also some objections to this use of resilience, chiefly by some of the MS. These objections have been pointed out earlier, in how they impede the coordinated response the EU wishes to achieve in this area through obstacles to information sharing.

Many of the functions of resilience are coordinated through the NIS-Directive and ENISA. However, this function rests on the assumption that transnational cooperation and thus coordinated responses in the face of cyber threats work as intended, including through cooperation between national NIS authorities and those at the EU level, working through ENISA.[263] However, one criticism that has been leveled at the EU conceptualisation of resilience is that it does not take into account certain differences in economic, social, historical, and security concerns of each MS, and therefore also not how perceptions of CS resilience might differ on a state by state basis.[264]

This also highlights the state centric issues of CS in this context, and also provides a counterpoint to the liberal institutionalist approach taken by the EU in the EUCSS and the NIS-Directive. Furthermore it also points to the difficulty of an institutionalised conceptualisation of security through the resilience concept in the EUCSS. Based on the examples provided in this context, the problem areas relate to instances where the MS have different conceptualisations of security than the one proposed in the EUCSS.

Moreover, the realist perspective can add to this perspective by analysing instances where MS act as security-seeking units in cyberspace, and merge traditional ideas of security with that of CS. In this case, the sovereignty issues associated with information sharing and coordination through the cyber resilience concept in the EUCSS point to instances where these states treat CS as a form of national security. However, in order to further analyse this phenomenon, the next

[263] Ibid, pp 5-6

[264] George Christou, *Cybersecurity in the European Union.*(Basingstoke; New York: Palgrave Macmillan, 2016)., p 63

section of the analysis will look at the individual MS cases, where it can be argued that state security perceptions of CS differ from the collective security espoused in the European strategy.

In sum, the liberal institutionalist approach becomes apparent in the EUCSS framework through the structure of the strategy that incorporates aspects of complex interdependence, as seen in the multiple channels of contact in the policymaking process of the strategy. In this regard, non-state actors have proven to serve as an influential point of contact in the procedural aspects of the EUCSS policies, such as the construction of norms and principles, based on the current internet architecture and the political as well as economic principles associated with this.

In addition, non-state actors are also involved in the current policies of the EUCSS and the NIS-Directive. Thus, it becomes apparent that the European strategy seeks to establish a collective sense of CS that largely incorporates non-state actors, who MS are in contact with through coordination of CS strategies and information sharing on cyber capabilities. This represents a form of complex interdependence where CS is negotiated through multiple channels of contact. The liberal institutionalist perspective would assert that this increases interaction between actors, which is evidently what has taken place in the EUCSS through the enactment of the NIS-Directive. This is exemplified by the use of and coordination of CERTs across MS and ENISA.

It can also be observed that the EU seeks to establish a collective sense of security through these liberal institutionalist principles that seek to grant equal attention to the issues from the public and private sectors. The second perspective that has been analysed here has been the use of cyber power. This relates to the interaction between the organisations and ICT providers working with the MS on security issues in the EUCSS. This involves specific forms of cyber power, which these non-state actors and MS are involved in and use to define their interests. From the non-state actor and EU institutional perspective, this is defined by the political interests embedded in the internet architecture, in the form norms and principles regarding rule-sets for IP addresses, and other internal factors of CS.

In relation to the EUCSS, the institutional cyber power is utilised by the practices in the strategy that seek to instill a liberal institutionalist type of behaviour through cooperation on CS issues, and the practices involved with that. Furthermore, structural cyber power is arguably also influential in this regard, as the EUCSS reflects the competitive logic of capitalism, when it is referenced that innovation and drive for growth in the private sector is a primary component of

CS in the European strategy. The MS also use cyber power through intermediary institutions, as observed in the state level political processes that have sought to influence policymaking in the EUCSS. This is another important factor to consider when analysing the individual CS strategies. The sub-conclusion of this section can be divided into the following points:

The UK Cyber Security Strategy

In this section the national CS strategy of the United Kingdom will be scrutinised based on its provisions related to cooperative elements and international engagement, outlined in the strategy. The aim is to extrapolate the established cooperation and conflict dimensions embedded in the strategy and relate these factors to the EUCSS. This allows an analysis of the areas where the U.K follows the liberal institutionalist approach adopted by the EU strategy, but also instances where it is argued that the U.K strategy diverts to pursue a realist approach to its CS strategy, mixed with applications of cyber power.

The U.K CS represents a significant case due to its policy influence on the European development of the EUCSS, seen through the proceedings of the London Conference, where the U.K has been involved multilaterally with the EUCSS in which it has also attempted to influence the framework with its own voluntary "meta-governance of identities"[265] approach, acting as a policy entrepreneur, and taking on a leadership role in European CS.[266] This approach also makes an important distinction between its own approach and that taken in the NIS-Directive. This type of approach has been contrasted with the hands-on approach in the NIS-Directive where there are now mandatory mechanisms in place for CS cooperation.[267]

This factor in the NIS-Directive is something that has been opposed by the U.K government who has been concerned about trust-building through a framework that imposes reporting of CS related incidents.[268] Instead, the market-based approach under the U.K government has called for informal relations, focusing on building trust within a CS framework

[265] Ibid, p 80
[266] Ibid
[267] Ibid
[268] Ibid

over time. In this case, it has been suggested that "mature" CS MS, such as the U.K. have preferred these informal engagements, rather than mandatory reporting.[269] With this factor in mind, the analysis of the British CS strategy can also take this into account, in relation to how this plays into the cooperation and conflict dimensions, and thus the possible problem areas identified with constructing an EU notion of collective security within the EUCSS. Furthermore, the analysis will also look at how notions of national interests and sovereignty are included in the UK strategy, and how this fits into the mold of the EUCSS.

In the main document of the strategy, an outline states the goals of the strategy as such:

> "Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society."[270]

In connection with the overarching strategy, four objectives are listed with the specific purpose of achieving the stated goals. In the first objective, the strategy mentions that the UK will tackle cyber-crime, with the intended effect of having the most secure place in the world to conduct business through cyberspace.[271] This objective shows a similar market-based approach to CS taken in the EUCSS, with the link between freedom and prosperity, as well as connecting threats from cyberspace to economic threats.[272] Thus underpinning notions of CS with a liberal logic, concerning the economic character of CS. However, it can also be argued that this is where it diverts from the European strategy which seeks to establish a collective sense of CS through the liberal institutionalist approach, with an emphasis on transnational cooperation, as part of the NIS-Directive.[273]

[269] Ibid
[270] Appendix 3, p 8
[271] Ibid
[272] Appendix 1, p 4
[273] Ibid, p 6

In relation to this statement, there is also a distinction between cyberspace as one informed by the theoretical application in this thesis. That is, cyberspace as an all-encompassing cyber-archipelago that consists of borderless computer systems.
However, it can be argued that the term is applied differently in this context, as seen in how the UK strategy describes the UK as a physical space in cyberspace, through how it aims to make it a secure place for business. From this perspective, the strategy sets out to delineate a safe cyberspace as something inherently based on the UK specific values described in the aim of the strategy. In this regard, a dichotomy arises between the core values guiding the UK strategy, with the concept of resilience as stated as one of the main CS principles in the EUCSS.[274] On one hand the UK strategy states that it will pursue resilience as part of its strategy, but on the other hand, its actions related to CS concerns are guided by national security.[275] This leads into the second objective outlined in the strategy, where it is also mentioned that the UK wishes to be resilient against cyber threats and attacks, but also protect their interests in cyberspace.

When contrasting the cocenpt of resilience between the UK strategy and the EUCSS, there are arguably discrepancies between the uses of the concept in question. First of all, when looking at the use of resilience in the EUCSS, the references to resilience are connected to ideas of cross-border cooperation between private and public sectors.[276] Moreover, this type of resilience relies on an information sharing network, where the national NIS authorities are expected to participate in cooperation throughout the EU.[277] Importantly, the provision of resilience also rests on the ability to carry out coordinated responses in relation to cross-border cyber threats.[278]

In the UK strategy, the concept of resilience is employed in a different context. This goes back to the connection between resilience and protection of interests in cyberspace. Therefore the EUCSS does encourage MS to develop their cyber defence policy, and thus increase resilience between communication and information systems to protect issues of related to their national security.[279] On the other hand, the UK strategy connects the development of resilience to national

[274] Appendix 1, pp 4-5
[275] Appendix 3, p 8
[276] Appendix 1, p 5
[277] Ibid, p 6
[278] Ibid, p 5
[279] Ibid, p 11

procedures, however, also referencing the testing of these procedures with international partners throughout the EU. Here, the strategy also refers to the resilience of organisations who are seen as a priority for the UK economy.[280] In this connection, the strategy also refers to national interests as guiding the capability building in cyberspace for the government.[281]
The two perspectives on CS and resilience as a central theme to the strategies thus show two different approaches to CS. The EUCSS is evidently caught between ensuring a certain level of harmonisation and cooperation between the CS strategies, but also promoting its own values in cyberspace among MS and countries outside the Union.[282] The UK strategy sees concepts as resilience and protection of interests as something that applies to British national interests, and for instance relevant to the UK economy.[283] This also brings up the notion of CS as a contextual issue, where national interests in cyberspace can be regarded as noteworthy in regards to capabilities.

For instance, these national interests are elaborated upon as information gathering interests, military and civilian capability building, and certain capabilities to preserve sovereign capabilities in "niche areas."[284] This arguably also shows a realist security approach to CS taken by the UK strategy. While the EUCSS defines its strategic areas and measures for security through a liberal institutionalist framework, these are primarily referenced in the UK strategy through references to national interests being the primary motivator for its CS provisions.

The realist theoretical perspective underpins these provisions through the conceptual use of power, which can appropriately be reflected in the UK strategy. For instance, it becomes clear that the UK approach acts as a security-seeking unit in its relationship with CS. This phenomenon is arguably present here, with the core motivations for the strategy pertaining to national programmes and capabilities for what the strategy considers appropriate to its aim.[285] Furthermore, the provisions outlined in this strategy also reflect the UK government as acting through principles of self-help from a realist theoretical perspective, especially in relation to its

[280] Appendix 3,. p 39
[281] Ibid
[282] Appendix 1, p 15
[283] Appendix 3, p 39
[284] Ibid
[285] Ibid

capability building as a measure to protect sovereignty.[286] One can then ask why the UK engages in cooperation with the European Strategy while simultaneously referring to its own political processes as a means of promoting international norms in cyberspace.[287] There is a possible way to explain this from the realist perspective, which relates to why states find it useful to engage in these cooperation initiatives under CS. In this regard, the institutions on their own provide a venue for states to further their own national interests. As a consequence, the UK strategy establishes this double-path by implementing the NIS-Directive, but following the national interests through the London Conference.[288]

The realist perspective would thus account for this as security being a form of relative gain, which the state can utilise to gain an advantage over other states. This is further related to the realist notion that states seek to maintain autonomy in an anarchic cyberspace, with a high distribution of power among transnational networks and private organisations. From this perspective, the UK can leverage national interests through the London Conference, and thereby also influence the policymaking process in the EUCSS.

Other work has also demonstrated how the UK perceives areas of cyberspace as a fundamental threat to its national sovereignty, as witnessed by its various specialist units, who have the purpose of identifying threats to its entities and interests.[289] This factor might also then account for the double-path taken by the UK in relation to its London Conference and recognition of the EUCSS. That is, through its own notion of security on top of the CS used by the EUCSS strategy. In this way, the UK has attempted to influence international norms on governance in relation to CS. However, as it has been noted, this has not led to broadly recognised norms or consensus on CS norms.[290] Despite the lack of consensus based on the London Conference, it still shows an attempt by a state to shape CS institutions, based on its own values. Moreover, this process has also led to informal CS agreements between the UK and other nation states such as China. On the other hand, this approach has reflected the UK approach to

[286] Ibid
[287] Ibid, p 40
[288] Sarah Backman and Magnus Ekengren, The Institutionalization of Cybersecurity Management at the EU-Level, p 43
[289] David J. Betz and Tim Stevens, "Power and cyberspace," *Cyberspace and sovereignty* 51, no. 424 (November 30, 2011): , accessed February 18, 2017, doi:http://dx.doi.org/10.1080/19445571.2011.636954., p 65
[290] George Christou, *Cybersecurity in the European Union.*(Basingstoke; New York: Palgrave Macmillan, 2016)., pp 79-80

CS within Europe as well, which is what has conflicted with the hands-on approach in the EUCSS through the NIS-Directive.[291]

In relation to the EUCSS, there has thus been disagreements about the approach to CS, specifically due to the trust-based reporting requirements in the NIS-Directive.[292] The UK government insists on the informal procedures as more viable for building trust between CS entities, and thereby increasing effective cooperation. Instead, it envisions a voluntary approach among MS, as noted in a study on the strategy.[293] The cyber power perspective can also be useful here to highlight the actions taken by the UK government in its CS strategy. The process in question follows the usage of institutional cyber power, as evidenced by the attempt to shape norms on CS both externally, but also internally within the EU, based on its own values in CS.

Therefore, this depicts the UK conceptualisation of CS and application of resilience in a different light than what has been applied in the EUCSS and the NIS-Directive. In the UK strategy this becomes apparent through the hands-off market governance approach to CS, as well as its emphasis on using this approach throughout its various pillars in its CS strategy.[294] This is in stark contrast to the NIS-Directive that utilises a formal approach, in the form of mandatory mechanisms.[295] Thus, the obstacles to the cooperation between the two strategies can be highlighted by not only the different approaches to CS and cooperation therein. But also the state interests the UK government have pursued in cyberspace, as it seeks to protect its national sovereignty in cyberspace. This includes certain values tied to the government's interpretation of CS, which is then carried out in its external policies through the London Conference.

Having analysed the UK strategy, the following sub-conclusions can be made concerning the alignment of the strategy in question and its cooperation and conflict dimensions with the EUCSS. In relation to the cooperation dimension, it can be deduced that while the UK strategy shares similarities with the EUCSS in its liberal institutionalist approach to areas of its CS, such as the focus on international cooperation and cooperation with non-state actors, there are still key differences in its framework related to CS, and thus how it links to the notion of collective security established in the EUCSS. The liberal institutionalist framework is present in the

[291] Ibid, p 80
[292] Appendix 2, p 9
[293] George Christou, *Cybersecurity in the European Union.*(Basingstoke; New York: Palgrave Macmillan, 2016)., p 80
[294] Ibid, p 84
[295] Ibid, p 85

representation of the CS provisions related to public and private sector cooperation, where both strategies emphasise the importance of interaction across state and non-state actors. Primarily in the form of ICT organisations in this case.

This is also where the theory of complex interdependence can help explain the inclusion of actors involved in the policymaking of the CS strategy. For instance, in the UK strategy, it has been pointed out that actors in the form of private organisations, but also intermediary institutions in the form of the London Conference have had a significant influence on provisions related to interests and embedded values in the CS strategy.

Limits to this theory have also been identified in the strategy. For instance, it does not sufficiently explain why national institutions (such as the London Conference) have had considerable influence on the strategy vis-á-vis supranational agreements on CS (the EUCSS and NIS-Directive). However, one aspect of this could also be due to the UK strategy being released before the official implementation of the EUCSS in 2013, and subsequently the NIS-Directive in 2016 On the other hand, the UK strategy does recognise the EU initiative in its strategy, but does not directly recognise the EUCSS and NIS-Directive in its external CS policy.[296]

This is where the realist theory can elucidate some of the provisions in the UK strategy, but also actions taken in regards to securing their interests in cyberspace. Here it is also important to mention that the UK has acted as a policy entrepreneur in key areas of the EUCSS and the NIS-Directive, through the London Conference on Cyberspace, and from this it can be argued that while the UK strategy formally recognises partnership with the EUCSS and formally recognises the NIS-Directive, there are also areas/provisions where the UK strategy clearly references national interests and sovereignty, as pointed out earlier. It is especially in regards to implementation of the EUCSS provisions in the NIS-Directive, where the two strategies diverge. This is further evidenced by the London Conference, where international norms of acceptable behaviour are within the confinement of this arrangement, are referred to as part of the strategy's vision of cyberspace. Therefore cyber power is also present throughout the provisions related to international cooperation in the strategy. It has been demonstrated that institutional cyber power, and the presence of intermediary institutions, such as the London Conference have played a significant part in ensuring that the values enshrined in this strategy, are promoted in the external policy of the UK strategy.

[296]Ibid, p 40

Following this, it can be argued that the UK strategy has followed its own interpretation of CS, which contradicts the EUCSS notion of CS, and also shows disagreement with aspects of the NIS-Directive. The analysis of this strategy through a pragmatic IR theoretical approach has identified areas of cooperation between the UK strategy and the EUCSS, but also identified areas where national interests and concerns of sovereignty underpin the values and goals of the UK strategy. The general problematisations of the NIS-Directive have also been identified in other work, thus increasing the validity of this analysis.[297]

Cyber Security Strategy for Germany

This section will analyse the German CS strategy and compare and contrast its provisions with the EUCSS and the NIS-Directive. The aim is to assess how the national strategy conceptualises CS in comparison with the European strategy.

The German strategy is essentially divided into two levels of control between the civilian aspects of the strategy and provisions controlled by the Bundeswehr/German army, in relation to Germany's preventive security strategy.[298] In the context of this, the strategy lays out framework conditions that drive the strategy itself, including the recognition that a mix of domestic and international policies are required to strengthen CS, due to the interconnected nature of cyberspace.[299]

As a consequence, the strategy employs a liberal institutionalist framework to its CS approach through cooperation with international entities, and shared responsibilities between the private sector, state, and civil society.[300] In this way, the strategy employs a similar approach to the EUCSS in regards to the cooperation mechanisms. This also mirrors the aspects of complex interdependence, in the form of institutionalisation taking place through multiple channels of contact, as evidenced by the inclusion of transnational and national actors in the

[297] Nicole van der Meulen, Eun Jo and Stefan Soesanto. Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Santa Monica, CA: RAND Corporation, November 18, 2015. https://www.rand.org/pubs/research_reports/RR1354.html.
[298] Appendix 4, p 3
[299] Ibid, p 2
[300] Ibid

institutionalisation process of the German strategy.[301] In this context, the strategy recognises the importance of international institutions, including the EU, NATO, and the Council of Europe among others, thereby also highlighting the importance of institutions in CS strategy. In connection with this, the strategy asserts its aim in this area is to "ensure the coherence and capabilities of the international community to protect cyberspace."[302]

The question that arises from this aim is then what can be considered coherence and capabilities from the German perspective. Hence, it is appropriate to assess the strategic objectives outlined by the strategy, in order to analyse how CS is conceptualised from this perspective.

The strategic objectives in the German strategy are outlined as ten different strategic measures and objectives. However, the analysis focuses on how the strategy frames the objectives related to national interests, sovereignty, and cooperation as motivating factors for the strategy itself. The third objective in the strategy refers to provisions with the purpose of strengthening IT security in the German public sector.[303] Here, it is interesting to note the emphasis on the state authorities as "role models for data security."[304] Although, the private sector is also considered crucial for information sharing in the first objective relating to protection of critical information infrastructures[305], there is still a state centric emphasis on data protection in this regard. This is for instance demonstrated by the top-down state-centric approach taken to data protection in this strategy, where there is an emphasis on having powerful structures within the German federal authorities to deal with CS related issues.[306] For this reason, the strategy emphasises governmental control on CS through different federal offices, while still also recognising international initiatives such as the Council of Europe Cyber Crime Convention as well as cooperation through ENISA.[307]

However, it is also in the international coordination objective of the strategy, where national interests are side-lined with the international collaboration on CS. It is explicitly mentioned that the German government will pursue German interests, as well as ensuring that its

[301] Ibid, p 3
[302] Ibid
[303] Ibid, p 4
[304] Ibid
[305] Ibid, p 3
[306] Ibid, p 4
[307] Ibid, p 5-6

own ideas of CS are coordinated and pursued within the various international organisations, including the Council of Europe and NATO.[308]

Thus from the IR perspective, the strategy presents two diverging approaches to CS. Having covered the liberal institutionalist aspects of the strategy, it can also be argued that the German strategy approaches CS from a realist state-centric perspective in regards to its external policy, as well as use of cyber power. The realist perspective becomes apparent through the emphasis on pursuing national interests and ideas on CS through international institutions. Yet, it is also interesting to note the insistence on these interests being pursued through international institutions. One can argue that this is an example of institutional cyber power, where cyberspace is utilised as a form of transnational communication to further domestic interests in the international domain.[309]

On the other hand, the realist approach from a CS perspective can also take this into account. One way of looking at this is how institutions become gateways for these national interests in the German strategy, and thus an extension of the national CS strategy through institutions.

However, this is arguably another point where the theoretical application of IR clashes with the data presented in the German strategy. On one hand, the strategy emphasises international cooperation, which can be explained through the IR lens of liberal institutionalism, as it takes into account the inclusion of state and non-state actors in this form of CS.

On the other hand, the strategy then mixes in elements of realism in its external policy, but even this form of cooperation involves recognition of other institutions, such as the European CS institutions. In addition, the strategy also recognises the need for a multilateral approach, combined with what it deems to be a "necessity of sovereign evaluation and decision-making powers."[310] Thus, the reality of this CS approach also shows some limitations to the IR perspective on CS, as it may account for the individual decisions taken in cyberspace by states and organisations, when analysed in isolation of one another.

However, when it is applied to the overall German CS strategy, discrepancies in the IR theoretical perspective can be found through the mixed use of realist and liberal institutionalist

[308] Ibid, p 6
[309] Ibid
[310] Ibid

approaches to CS. This is additionally evidenced by the reference to NATO as the basis for transatlantic security, and therefore also CS as one of its responsibility areas.[311] Using the realist perspective in accordance with the CS literature, this could be explained by the fact that Germany is still retaining its own strategy, despite recognising CS cooperation with NATO.[312]

In addition to this, the German government is also in possession of its own cyber army, with the purpose of solidifying its capabilities in cyberspace, in the form of defensive and offensive capabilities.[313] In this connection, the head of Germany's Federal Office for the Protection of the Constitution, Hans-Georg Massen, has stated that Germany should not only focus on protecting digital infrastructure, but also possess offensive cyber capabilities to counter future attacks. Following this statement, the intelligence chief also states that his agency should have clearer regulations for countering these attacks, and thus protect the German CS.[314] This would for instance account for Germany as a security-seeking unit in cyberspace, through the development of cyber capabilities.

While this factor can be taken into account from the realist perspective, when cyberspace is viewed as a system of anarchy, and therefore the German government must extend its security apparatus into this domain, there are also limitations to this realist proposal. For instance, the strategy refers to German technological sovereignty and economic capacity, as something that must be strengthened, but also areas, where they will pool their resources across Europe, and share technology.[315]

This arguably shows a wish for institutionalised reciprocity in the German strategy, and therefore diverts from the realist perspective that treats CS as a form of capability building in cyberspace, and an extension of information warfare. Therefore this shows another digression from the realist perspective to a liberal institutionalist perspective.

Nonetheless, the aforementioned provisions still exemplify elements of both IR theoretical perspectives. Yet, in the overall context of the strategy, these areas of national

---

[311] Ibid, p 7

[312] Miguel Alberto Gomez, "Identifying cyber strategies vis-a-vis cyber power,", p 2

[313] "Germany rolls out new cyber defence team," EURACTIV.com, April 06, 2017, , accessed May 20, 2017, https://www.euractiv.com/section/cybersecurity/news/germany-rolls-out-new-cyber-defence-team/.

[314] Philip Oltermann, "Germany's spy chief calls for counterattacks against cyber-enemies," The Guardian, January 10, 2017, , accessed May 15, 2017, https://www.theguardian.com/world/2017/jan/10/germany-spy-chief-hans-georg-maassen-calls-for-counterattacks-against-cyber-enemies.

[315] Appendix 4, p 7

interests and institutional cooperation are applied in a complementary context, exemplified by the strategy's aim to merge sovereign evaluation and decision-making powers with a multilateral approach.[316]

In relation to these factors, the German strategy also emphasises the role of the government to ensure CS, which is linked to freedom and prosperity. Furthermore, these values are linked to successful international cooperation on CS and thus securing cyberspace.[317] Once again, national interests, in the form of security and economic values, are tied to international cooperation on CS. Thus, it presents a seemingly blended IR theoretical perspective on the core issues identified in the German strategy.

However, this is arguably also where theoretical understandings of CS can help explain this environment, and why the German strategy is characterised as such. One area that can be identified in this regard, is the borderless nature of cyberspace and thus also CS.

Therefore, this also challenges the realist perspective on security, despite the German government acting as a security-seeking unit in references to pursuing national security interests in its external policies.[318] On the other hand, this notion of security is limited by the recognition in the strategy that states: "in global cyberspace security can be achieved only through coordinated tools at national and international level."[319] The German approach to CS can thus be described as a mix between domestic policies and international collaboration on specific security issues. It is important to note that recognises cooperation with the EUCSS, on CS related to critical information infrastructures.[320] However, there is no direct mention of transnational public-private cooperation in relation to the EUCSS, and therefore also no reference to the resilience concept used by the EUCSS in this regard. Instead, this form of cooperation takes place through the federal government.[321] Thus, there are also issue areas, where the German strategy insists on maintaining certain issue areas within its federal offices and the National Cyber Security Council.[322] Therefore there are still areas, where the strategy maintains sovereign control of what it deems to be national interests. This might also provide an explanation as to

[316] Ibid, p 6
[317] Ibid, p 8
[318] Ibid, p 6
[319] Ibid
[320] Ibid
[321] Ibid, p 5
[322] Ibid

why other literature has pointed to the German strategy as taking a double-path approach to the EUCSS,[323] coupled with the aim of the external policy to pursue these interests internationally. Nonetheless, there is also one other alternative explanation to the discrepancy between the German strategy and the EUCSS.

Based on the aforementioned factors, it can be argued that the IR theoretical perspective can analyse the individual provisions in the strategy, and thus relate them to their realist and liberal institutionalist perspectives. In doing so, it is also possible to connect these to the cooperation and conflict dimensions. The realist perspective can account for the state-centric actions taken by the German government through its external CS policies. Moreover, specific provisional areas in the strategy emphasise a top-down state approach of CS issues through federal offices. In addition, the strategy is complemented by the German preventive security strategy, run by the German armed forces.[324]

It can be argued that this part of the strategy fits the conflict dimension as the domestic interests involved in the external policy, combined with the wish to pursue these in international institutions, conflicts with the EUCSS. As mentioned earlier, the EUCSS and NIS-Directive formally recognise the national MS strategies. Although, the logic of the NIS-Directive also requires the MS to cooperate within the mandatory provisions, as covered earlier. The pursuit of German interests in its external policy might for instance conflict with the good practices outlined in the EUCSS. Though, this would also require insight into the specific national interests pursued in the international organisations.

The liberal institutionalist perspective does account for the strategy's recognition of international cooperation and private-public sector interaction. In sum, the German strategy evidently employs a mix of domestic and international approaches to CS. In order to adjust the strategy to the framework of the EUCSS, the aforementioned factors must then be taken into account.

[323] Sarah Backman and Magnus Ekengren, The Institutionalization of Cybersecurity Management at the EU-Level, p 43

[324] Appendix 4, p 3

French National Digital Security Strategy

The national CS strategy of France serves to further elucidate the EUCSS conceptualisation of collective security under its CS strategy. Thus the primary analysis will look at the outlined provisions in relation to cooperation aspects and international engagement in the French strategy. Through this analysis, it will be shown how the strategy employs a combination of liberalism, realism, and cyber power in its policies, and what these theories might say in relation to the French conceptualisation of CS.

The French strategy is divided into five strategic objectives, pertaining to state interests, digital privacy, CS training, private policies, and finally CS in Europe, digital strategic autonomy, and cyberspace stability.[325] The object of the analysis, however, focuses primarily on the state interests, private sector aspects, and the international engagement, as these are the points that inform the focus of the analysis - that is, related to the concepts of national interests and sovereignty which are included in the cooperation and conflict dimensions.

First of all, the French strategy states the first objective as: "France will ensure the defence of its fundamental interests in cyberspace. It will reinforce the digital security of its critical infrastructures and do its utmost to ensure that of its essential operators to the economy."[326] The first part that is interesting to the analysis, is thus how these fundamental interests are defined, and how they relate to the notion of cyberspace in this strategy. In this connection, the orientation toward this goal is the development of scientific, technical, and industrial capabilities that will help protect what the strategy regards as sovereign information, CS, and a trustworthy digital economy.[327] In this part of the strategy, a liberal institutionalist approach is applied to organising its CS priorities through what the strategy refers to as the "Expert Panel for Digital Trust."[328] This utilises a multistakeholder approach, incorporating both the state authorities and private sector in its strategy. This also further reinforces the presence of multiple channels of contact in CS, as it displays a form of fragmented state authority in the area

[325] Appendix 5, p 5
[326] Ibid, p 14
[327] Ibid, p 14
[328] Ibid

of CS, where these state authorities in the form of ministries share competences with private organisations.[329]

However, it also becomes clear that the French government approaches this setup, with a degree of apprehension to the private sector. This becomes evident in the statement that the choices of major private stakeholders can either "consolidate trust or incite mistrust."[330] Although the strategy initially outlines a liberal institutionalist model, based on increased interaction between the French governmental authorities and private sector in the IT-sector, there are also apparent limits to this theoretical perspective in this regard.

In this connection, the French government maintains a state-centric approach to the area of cooperation with private sector stakeholders, by economic and technological monitoring through the expert panel.[331] This can also be contrasted against the hands-off market approach taken by the UK government, where it has been noted that it is primarily the private sector that informs the state on CS-related issues.

Therefore, while the liberal institutionalist model can be applied to both cases, the data presented here also highlights the different degrees of government involvement and interaction with the private sector. Thus, it can also be pointed out that CS is contextual in this regard, as there may be elements of liberal institutionalism present in this particular CS strategy, such as contact between the private and public sector.

On the other hand, the degree of this relationship is arguably contextual to the area of CS, as the state itself seeks to control CS from a top-down approach, where the input of the private sector is arguably determined by the state through its expert panel.[332] From the perspective of the French government, this form of conceptualisation is further evident in their approach to information systems, where the strategy mentions the protection of "sovereign information."[333] This is mentioned in relation to certain state focused measures aimed at providing government and military capabilities, with the purpose of preserving autonomy in decision-making.[334]

[329] Ibid, pp 14-15
[330] Ibid, p 15
[331] Ibid
[332] Ibid
[333] Ibid
[334] Ibid

This further elucidates the mixed approach in the French strategy, as one hand it, it combines elements of complex interdependence, where CS is viewed from an economic perspective that is negotiated by state and non-state actors, as evidenced by administrative duties being divided between the ministries and private sector.[335] Yet, it also evident that information is regarded as a sovereign provision in the strategy, and directly related to the aforementioned government and military capabilities.[336] Thus, in order to account for the mix of these two approaches, it would be valuable to consider the context of CS specific issues that have been raised in the literature.

This for instance points to the role of information in complex interdependence in the information age. From this point of view, it can be argued that the French government perceives sovereign information to be a particular type of strategic information. Often referred to a form of asymmetrical type of information, the strategic information can thus encompass military capabilities. In relation to the strategy, it is mentioned that these measures to protect sovereign information are aimed at the government and military to provide specific capabilities that can then aid autonomous decision-making for the government.[337] Thereby, this type of information also connects to the conceptualisation of strategic information as a form of capability that confers an advantage to the actor in possession of it.

Thus, it also connects this form of CS to the traditional IR perspective on security. On one hand, CS is used as a form of shared competence between a plethora of actors in the French context, but it also connects to a more fundamental debate, on for instance realism. That is, it can be argued that the maintenance of autonomy is highly prioritised in the French strategy; therefore cyber capabilities to protect its sovereign information follow the logic of fundamental distrust in CS. It can also be argued that this factor is heightened when taking into account the asymmetrical nature of threats in cyberspace. In this sense, compulsory cyber power can also serve as a concern when states seek measures to protect sovereign information in cyberspace, as they can be threatened by asymmetrical powers in the form of non-state actors, with access to cyber capabilities. E.g. these actors could gain access to the information of a state and attempt to perform coercive actions through compulsory cyber power.

[335] Ibid
[336] Ibid
[337] Ibid

This also serves a challenge to the state unit, when taking into account that cyberspace can be regarded as borderless. In relation to the French government, concerns about these asymmetrical forms of power have been raised in the 2017 French election. In this case, fears about Russian interference through the use of bots to sway political opinions, were raised by the French intelligence agency.[338] Thus, compulsory cyber power can be perceived as a threat to the state in areas where information can be used against it. Therefore, while the setup of the French strategy entails a liberal institutionalist approach, there are evidently also areas where the French government acts as a security-seeking unit, as power becomes more intangible due to these asymmetrical threats in cyberspace. In addition, the French White Paper that has laid the foundation for its strategy states that cyber-related threats are included in the French defense strategy, together with nuclear deterrence. While the paper also recognises the importance of the international community in this regard, it also positions this approach to national security in the larger European defence policy.[339] Going forward, this is also an important consideration for how the strategy outlines cooperation on CS, due to this perception of claiming sovereignty in cyberspace.

The orientation of the strategy informs the international cooperative aspects of the strategy in several ways. This is accounted for in the strategy's reference to its multilateral engagement, where the strategy clearly references cooperation with ENISA and the European Directive (NIS) and intent to cooperate within this CS framework.[340] Hence, CS as a cooperative engagement and the need to secure information is also recognised, despite the perception of information in cyberspace also being considered a capability and sovereign in this regard, and thereby taking a realist approach to these interests in cyberspace.[341]

This line of approach is also underpinned by values of autonomous thinking, stated in the strategy as related to the post-Second World War environment of France, which in turn drives its approach to diplomacy. Here it is also mentioned that digital technology has changed French society, but the extent to which this affects concepts such as sovereignty, territory, and

[338] Emily Tamkin, "French Intelligence Agency Braces for Russian Bots to Back Le Pen," Foreign Policy, February 08, 2017, accessed May 5, 2017, http://foreignpolicy.com/2017/02/08/french-intelligence-agency-braces-for-russian-bots-to-back-le-pen/.

[339] France., Présidence de la République., Ministry of Defence., *White Paper on Defence and National Security* (Paris: Ministère de la défense, 2013), , 2013, accessed May 1, 2017, http://www.defense.gouv.fr/english/portail-defense., p 7

[340] Appendix 5, p 17

[341] Ibid

fundamental interests is still being considered by the government.[342] However, when looking at cooperation with European CS, the French strategy asserts itself as (along with voluntary MS) as the "driving force behind European strategic autonomy."[343] In this area, of the strategy, it can be argued that institutional cyber power is used to refer to its cooperation with the international community on CS. E.g. through how it asserts that it will use informal channels to discuss CS related issues, but also in how it seeks to reinforce its own presence on these international discussions.[344] Moreover, this form of cyber power is also apparent in the aim to assist in CS capability building, based on an approach building on partnerships.[345] In addition, the strategy refers to its partnership with Germany on cloud computing as setting standards within this area of CS.[346] However, there is for instance no direct reference to the cloud computing standards in the Directive in this case.

In the analysis of the French strategy, it becomes evident that the French strategy refers to a wider framework of European CS cooperation. Interestingly, however, the EUCSS and NIS-Directive are sparsely referred to. Instead, the strategy combines liberal institutionalist measures, in the form of interaction between public and private sectors, but also in the area of institutional measures for CS issues. In this case, the strategy also combines elements of structural realism in regards to information as a sovereignty issue. Although, this is not clearly defined by the strategy, it can be argued that if cyberspace is considered anarchic, then these uncertainties about information arise. This also goes back to the previously mentioned concern of alleged Russian hacking in the French elections.

If the lack of attribution and fundamental distrust is particularly significant in cyberspace due to lack of borders and actors with asymmetric cyber power, then this could explain the concept of sovereignty in relation to digital information. Thus these concerns could also reflect compulsory cyber power as a possible coercive element that might threaten sovereignty in this regard, combined with the factor that no physical borders prevent these asymmetric attacks. Based on this, these elements of cyber power can also provide a contextual explanation as to why the strategy takes these measures to protect sovereignty emphasise French values in cooperative

[342] Ibid
[343] Ibid, p 39
[344] Ibid, pp 39-40
[345] Ibid, p 40
[346] Ibid, p 39

engagements. This approach can also serve as an obstacle to establishing a framework of collective CS in the EUCSS, as the domestic values are prioritised in CS cooperation.

Sub-Conclusion of Analysis

Having analysed the respective CS strategies, the following points can be made in regards to cooperation and obstacles to the collective framework of European CS. While the selected cases all refer to the EU partnership in their strategies and to an extent follow similar liberal institutionalist approaches in connecting state actors and civil society on CS issues, there are obstacles present in the form of sensitive sovereignty issues pertaining to information sharing. The IR theories, together with the CS literature this illuminate the context where these issues can become obstacles to attempts at collective CS.

Liberal institutionalism can highlight the cooperative aspects of some cyber capabilities, such as institutionalising technological capabilities, as seen in the German case. Elements of structural realism can explain the conflict dimensions that arise from states asserting control over sovereign information and capabilities, if cyberspace is regarded as borderless, and consisting of asymmetric powers, as observed in the French strategy. Finally, cyber power can be demonstrated in one shape or form in all these strategies, as it functions as a manifestation of power in cyberspace, where actors seek security. As a result, cyber power can also serve as an obstacle to a collective CS strategy, as seen in some of these cases, where both state and non-state actors can challenge the sovereignty of a state, as observed in the French case.

Comparative Case Analysis of CS Strategies	Cooperation	Conflict
EUCSS/NIS-Directive	- Liberal institutionalist framework for information sharing - Recognition that MS are responsible for national strategies - Norm setting - Defines requirements for minimal cooperation	- Limits to information sharing with MS - MS lean toward voluntary approaches - MS define cyberspace individually - Structural cyber power may limit - Norms may conflict with MS interests/values
U.K.	- State functions as a security-seeking unit in CS - Market approach - Policy entrepreneur through London Conference - Formal recognition of international CS cooperation	- Hands-off market approach conflicts with mandatory NIS-Directive provisions - Refers to London Conference as guiding CS strategy - Institutional cyber power in international engagement
Germany	- Refers to EU initiatives on CS - CS as shared responsibility across state and non-state actors	- Emphasis on German values being pursued in international institutions - CS as a military capability
France	- Recognition of the Directive - Actively seeks international cooperation - Emphasis on MS sovereignty - Bilateral cloud computing cooperation with Germany	- French values pertinent to international cooperation - CS as a military capability - Own interests in the international sphere - Sovereign information, unspecified

Discussion

One additional perspective that would be useful as another avenue of research could for instance be the semi-constructivist perspective offered by Cavelty in the previous literature section. This could look at how threats are represented in cyberspace by states and institutions, as well as analyse exactly how certain CS related issues become securitised through discourse and actions. This may also provide an additional insight into how critical infrastructures become embedded in values of sovereignty and interests of the state, as discourses around CS is circulated increasingly in political debates.

Conclusion

Having analysed the selected cases of national CS strategies in conjunction with the EUCSS, together with an assessment of the theoretical perspectives, there are several perspectives that must be taken into consideration when analysing the obstacles to a collective framework of CS in Europe. In this regard, the EUCSS constructs its strategy through a liberal institutionalist approach that sets minimum requirements for cooperation through the legal text of the NIS-Directive. However, while the strategy seeks to harmonise CS among MS and emphasise economic benefits in regards to CS cooperation, these norms do not line up with the selected national strategies. While all three cases refer to cooperation with the EUCSS, provisions related to sovereignty, national interests, security, and international cooperation reflect individual approaches in these strategies are also reflected in these strategies, in some cases they also provide security challenges to the states in question, as they will have to balance the economic benefits that information technologies present in engagement with institutions, from a liberal institutionalist perspective.

The security questions become apparent in instances where sovereignty is involved, and in this connection, where asymmetric powers beyond the state borders may threaten digital information that is connected to the critical infrastructures, citizens, and other central features of these states. Therefore CS also presents a security dilemma, when taking into consideration that cyberspace both involves opportunities, but also challenges, as the digital borders of the states are permeated both by digital transnational flows of communication, but also the fragmented

monopoly in these state systems through non-state networks. Thus when considering the obstacles to a collective framework of CS in the European Union, it is arguably these contextual problematisations embedded in the national approaches to CS that are in limbo between the rapid introduction of information technologies, but also its security challenges, which in these cases, are met with capability building in the form of information warfare resources, or through use of cyber power as soft power to guide domestic interests in international institutions. Thus, in some cases these states apply state-centric defensive realism approaches to the security problems in cyberspace, either considering CS a capability or something that must safeguard their own digital information. In contrast, these states still emphasise the need for international cooperation, which leads to the question of when states consider it useful to engage with CS institutions from an absolute gains perspective. An insight into the social processes and for instance threat representations in CS could serve as a useful avenue of further research for this additional perspective.

Bibliography

"About ENISA." About ENISA - ENISA. June 24, 2016. Accessed March 12, 2017. https://www.enisa.europa.eu/about-enisa.

"Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace." Digital Single Market. February 07, 2013. Accessed March 10, 2017. https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-

"Cyber security directive held up in face of 'Wild West' Internet." EURACTIV.com. April 17, 2015. Accessed May 24, 2017. https://www.euractiv.com/section/digital/news/cyber-security-directive-held-up-in-face-of-wild-west-internet/.

"Cyber Security Strategy for Germany." Cyber Security Strategy for Germany - ENISA. February 20, 2014. Accessed March 12, 2017. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-strategy-for-germany/view.

"Cyber Security Strategy of the United Kingdom." Cyber Security Strategy of the United Kingdom - ENISA. February 20, 2014. Accessed March 15, 2017. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-strategy-of-the-united-kingdom.

"Cybersecurity." Digital Single Market. September 03, 2017. Accessed March 10, 2017. https://ec.europa.eu/digital-single-market/en/cybersecurity.

"France Cyber Security Strategy." France Cyber Security Strategy - ENISA. October 19, 2015. Accessed March 15, 2017. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf/view.

"Report on Cyber Crisis Cooperation and Management." Common practices of EU-level crisis management and applicability to the cyber crises. April 4, 2016. Accessed February 15, 2017. https://www.enisa.europa.eu/publications/eu-level-crisis-man.

"SCO," CCDCOE, September 07, 2015, , accessed May 2, 2017, https://ccdcoe.org/sco.html.

"The Directive on security of network and information systems (NIS Directive)." Digital Single Market. September 03, 2017. Accessed March 15, 2017. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

Backman, Sarah and Magnus Ekengren, The Institutionalization of Cybersecurity Management at the EU-Level, Master's thesis, Swedish Defence University, 2016 (Master's Programme of Politics & War)

Baldwin, David A., Neorealism and Neoliberalism: The Contemporary Debate (New York: Columbia University Press, 1993.

Bauer, Harry, and Elisabetta Brighi. *Pragmatism in international relations*. London: Routledge, 2009.

Baylis, John. *Globalization of world politics: An introduction to international relations*. Oxford: Oxford university press, 2011.

Betz, David J., and Tim Stevens, "Power and cyberspace," Cyberspace and sovereignty 51, no. 424 (November 30, 2011): , accessed February 18, 2017, doi:http://dx.doi.org/10.1080/19445571.2011.636954.

Betz, David J., and Tim Stevens. "Power and cyberspace." Cyberspace and the state 51, no. 424 (November 30, 2011): 35-54. Accessed February 18, 2017. doi:http://dx.doi.org/10.1080/19445571.2011.636954.

Bossong, Raphael, and Ben Wagner. "A typology of cybersecurity and public-private partnerships in the context of the EU." *Crime, Law and Social Change*, 2016, 1-24. doi:10.1007/s10611-016-9653-3.

Bryman, Alan *Social Research Methods*.Oxford: Oxford University Press, 2012.

Castells, Manuel. *The Informational city: Economic restructuring and urban development*. Oxford: Basil Blackwell, 1989.

Cavelty, Myriam Dunn, Mareile Kaufmann, and Kristian Søby Kristensen. "Resilience and (in)security: Practices, subjects, temporalities." *Security Dialogue*46, no. 1 (2015): 3-14. Accessed March 15, 2017. doi:10.1177/0967010614559637.

Cavelty, Myriam Dunn, Victor Mauer, and Sai Felicia. Krishna-Hensel. Power and security in the information age investigating the role of the state in cyberspace. Aldershot, Hants, England: Ashgate, 2007.

Cavelty, Myriam Dunn. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse." *International Studies Review* 15, no. 1 (March 2013): 105-22. Accessed March 20, 2017. doi:10.1111/misr.12023.

Christou, George. *Cybersecurity in the European Union*. Basingstoke ; New York: Palgrave Macmillan, 2016.

Deibert, Ronald J., and Rafal Rohozinski. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology* 4, no. 1 (2010): 15-32. Accessed March 20, 2017. doi:10.1111/j.1749-5687.2009.00088.x.

Demchak, Chris C., and Peter J. Dombrowski. "Rise of a Cybered Westphalian Age: The Coming Decades." Strategic Studies Quarterly 5, no. 1 (2011): 31-62. Accessed March 20, 2017. doi:10.1007/978-3-642-55007-2_5.

Denardis, Laura. "Hidden Levers Of Internet Control." *Information, Communication & Society* 15, no. 5 (February 16, 2012): 720-38. Accessed May 5, 2017. doi:10.1080/1369118x.2012.659199.

Eriksson, Johan, and Giampiero Giacomello. International relations and security in the digital age. London: Routledge, 2010.

Eriksson, Johan, and Giampiero Giacomello, " The Information Revolution, Security, and International Relations: (IR)relevant Theory?," *International Political Science Review* 20, no. 3 (2006):, accessed April 2, 2017, doi:10.1177/0192512106064462.,p 229

France. Présidence de la République. Ministry of Defence. *White Paper on Defence and National Security*. Paris: Ministère de la défense, 2013. 1-137. 2013. Accessed May 1, 2017. http://www.defense.gouv.fr/english/portail-defense.

Friis, Karsten, and Jens Ringsmose. *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*. London: Routledge, Taylor & Francis Group, 2016.

"Germany rolls out new cyber defence team," EURACTIV.com, April 06, 2017, , accessed May 20, 2017, https://www.euractiv.com/section/cybersecurity/news/germany-rolls-out-new-cyber-defence-team/.

Gomez, Miguel Alberto. "Identifying cyber strategies vis-a-vis cyber power." *2013 World Cyberspace Cooperation Summit IV (WCC4)*, November 2013, 1-7. Accessed May 5, 2017. doi:10.1109/wcs.2013.7050504.

Haaster, Jelle Van. "Assessing cyber power." 2016 8th International Conference on Cyber Conflict (CyCon), 2016. Accessed April 13, 2017. doi:10.1109/cycon.2016.7529423.

Herrington, Lewis, and Richard Aldrich. "The Future of Cyber-Resilience in an Age of Global Complexity." *Politics* 33, no. 4 (2013): 299-310. Accessed April 1, 2017. doi:10.1111/1467-9256.12035.
International Security 20, no. 1 (1995): 39-51. doi:10.2307/2539214.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no. 2 (2013): 7-40. Accessed April 20, 2017. doi:10.1162/isec_a_00138.

Keohane, Robert O., and Joseph S. Nye. "Power and Interdependence in the Information Age." Foreign Affairs 77, no. 5 (1998): 81-94. Accessed April 20, 2017. doi:10.2307/20049052.

Keohane, Robert O., and Lisa L. Martin. "The Promise of Institutionalist Theory."

Keohane, Robert Owen., and Joseph S. Nye. Power and interdependence. Boston: Longman, 2001.

Klimburg, Alexander. "Mobilising Cyber Power." Survival 53, no. 1 (January 28, 2011): 41-60. Accessed March 28, 2017. doi:10.1080/00396338.2011.555595.

Klimburg, Alexander, "The Whole of Nation in Cyber Power," *International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity*, 2011, , accessed March 29, 2017, http://www.jstor.org/stable/43133826.

Lamont, Christopher K. *Research methods in international relations*. Los Angeles: Sage, 2015. maassen-calls-for-counterattacks-against-cyber-enemies.

Meulen, Nicole Van der, Eun Jo, and Stefan Soesanto. "Exploring Cybersecurity Threats and Policy Responses in the EU and Beyond." RAND Corporation. November 18, 2015. Accessed March 13, 2017. http://www.rand.org/pubs/research_reports/RR1354.html.

Nye, Joseph S. Cyber power. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010.

Oltermann, Philip. "Germany's spy chief calls for counterattacks against cyber-enemies." The Guardian. January 10, 2017. Accessed May 15, 2017. https://www.theguardian.com/world/2017/jan/10/germany-spy-chief-hans-georg-

Powell, Robert. "Absolute and Relative Gains in International Relations Theory." The American Political Science Review 85, no. 4 (1991): 1303. Accessed April 12, 2017. doi:10.2307/1963947.

Simon, Stephanie, and Marieke De Goede. "Cybersecurity, Bureaucratic Vitalism and European Emergency." *Theory, Culture & Society* 32, no. 2 (January 14, 2015): 79-106. Accessed February 4, 2017. doi:10.1177/0263276414560415.

Tamkin, Emily. "French Intelligence Agency Braces for Russian Bots to Back Le Pen." Foreign Policy. February 08, 2017. Accessed May 5, 2017. http://foreignpolicy.com/2017/02/08/french-intelligence-agency-braces-for-russian-bots-to-back-le-pen/.

Tropina, Tatiana, and Cormac Callanan. Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. Cham: Springer International Publishing, 2015.

Tuthill, David Paul "Reimagining waltz in a digital world: Neorealism in the analysis of cyber security threats and policy," Ph.D. dissertation, University of Kent, March 2012.