The Threat of Digital Disinformation: A European Approach

Ellika Amundin
Abstract

The spread of disinformation on social media platforms has in the last few years gained much scholarly attention, in particular its ability to alter democratic processes. The focus of this thesis has however been on the discourse surrounding disinformation rather than disinformation itself, more precisely, the construction and perception of disinformation as a security threat. Disinformation is an issue which is rapidly evolving with the creation of new technologies and opportunities. The aim of this thesis has been to investigate if this has led to a shift in the perception of disinformation as a threat and therefore a change of policy for the EU. This was realised through the utilisation of Carol Bacchi's WPR approach toolkits, in combination with the foundational principles derived from securitization theory.

The thesis shows that the EU’s perception of disinformation as a threat has evolved from mainly focus on the decline of public trust and democratic processes. To also include and recognise a more multifaced view of the issue with a larger focus on manipulation, technology driven threats and media literacy deficiency.

Wordcount: 13378
**Table of Content**

1.0 Introduction ................................................................................................................................. 4

2.0 Literature Review and Theoretical Framework ........................................................................... 5
   2.1 Digital Disinformation as a Concept ................................................................................................. 6
   2.2 Digital Disinformation as a Security Threat ..................................................................................... 7
   2.3 A European Approach in the Fight Against Digital Disinformation ............................................. 10
   2.4 Theoretical Perspective .................................................................................................................. 11

3.0 Research Design ............................................................................................................................ 17
   3.1 What’s the ‘problem’ represented to be? ......................................................................................... 17
     3.1.1 Question 1 .................................................................................................................................. 19
     3.1.2 Question 2 .................................................................................................................................. 20
     3.1.3 Question 4 .................................................................................................................................. 20
   3.2 Operationalization ......................................................................................................................... 20
   3.3 The Data ....................................................................................................................................... 22
   3.4 Limitations and Potential Biases ................................................................................................... 23

4.0 Analysis ........................................................................................................................................ 23
   4.1 what’s the problem represented to be? ......................................................................................... 23
     4.1.1 Security of Ad Placement, Political Advertising and Issue-Based Advertising .......... 24
     4.1.2 Integrity of Services .................................................................................................................. 26
     4.1.3 Empowering Consumer and the Research Community ....................................................... 28
   4.2 Assumptions and Prepositions .................................................................................................... 29
   4.3 What is left unproblematic in this problem representation? Where are the silences? ...... 31

5.0 Conclusion .................................................................................................................................. 33

Bibliography .................................................................................................................................... 35
1.0 Introduction

In a time where information is more accessible than ever before, the issue of false information i.e., disinformation, misinformation, and fake news, has grown and received more academic attention. In particular, the spread of digital disinformation on social media platforms has caught scholarly attention which has become more notable after events where it could have caused biases on the outcome of political processes. Examples of such include the Brexit referendum and the 2016 US presidential election (Datzer & Lonardo, 2022). Thus, the dissemination of disinformation has in recent years been described as a threat to, mainly Western, democracy and security. However, the threat conception does vary from being described as an emotional weapon, used to threaten democratic processes (Wojczewski, 2021), to scholars who argue that it is in fact the strive to regulate disinformation that is the real threat to democracy i.e., a threat towards free speech (Monti, 2021).

The aim of this thesis is to understand this relatively new threat, and some of the problems surrounding it, by analysing the European Union’s (EU) approach to the issue. This will be done by looking at the EU and reviewing the EU’s Code of Practice on Disinformation, the first published in 2018 and a second “Strengthened” version in 2022.

The thesis argues and follows the framework that Digital disinformation is to be recognised as a social threat. Hedling (2021) and other scholars highlight the close connection between disinformation, the rise of social media, and the rapid dissemination of digital information. The works of researchers like Datzer and Lonardo (2022) further emphasise the perception of digital disinformation as a threat, solidifying the argument that it poses a social threat. This is due to its nature of spreading through discourse and its capacity to impact various aspects of society, such as shaping public opinion. Digital disinformation, in addition, is not bound by specific materialistic or geographical constraints but rather exists in a constant and universal manner. It invades online spaces and transcends traditional limitations of time and physical boundaries, making it a multifaceted and pervasive challenge in today’s digital age. The focus of this thesis is thus on the discourse surrounding disinformation rather than disinformation itself, more precisely, the construction and perception of disinformation as a security threat. Disinformation is however an issue which is rapidly evolving with the creation of new technologies and opportunities. The aim of this thesis is to investigate if this has led to a shift in the perception of disinformation as a threat and therefore a change of policy for the EU. The research question will thus be:
How has the EU’s perception of disinformation as a threat evolved/changed between 2018 and 2022?

Disinformation is in no regard a traditional security threat, such as threat of armed conflicts. In other words, it is an abstract concept formed through words. To be able to provide answers to the research question guiding the process, a critical security studies approach is taken to the investigation. The methodological tools appropriated in this study are selected from Carol Bacchi’s What’s the Problem Represented to be (WPR) approach. The theoretical ideas and core concepts of securitization theory guides the process of interpreting the relevant data found, developed by the Copenhagen School (Buzan et.al, 1998).

For the remainder of this thesis, the second chapter is divided into four sections and will in different themes review the previous literature deemed relevant and discuss the scholarly findings as well as their contributions to the question in focus. Chapter three will present and discuss the data analysed in this thesis, the methodological toolkit used to do so, and any potential limitations in the research. The fourth chapter will present the findings and analyse them with the help of the theoretical framework of securitisation theory appropriated. The last chapter will present the conclusions as well as the key arguments found of relevance to answer the proposed research puzzle.

2.0 Literature Review and Theoretical Framework

Considering the spread of disinformation and populism in political spheres in the 21st century, the second chapter of this thesis will present and discuss the relevant literature and studies already conducted by scholars in the field. It is divided in four sections which all help the thesis in addressing the research puzzle and later answering the research question. The focus of this thesis is to identify if there has been a shift in the EU’s threat perception and if the organisation views digital disinformation as a bigger threat in 2022 than it did in 2018 through a comparative approach. The literature will thus focus on disinformation within the realm of the EU, both how it operates and the potential dangers of it, as well as the EU’s approach in combating it.

The first section will discuss the concept of digital disinformation and narrow down the meaning behind this often broadly applied term. The second section will focus on how digital disinformation on different levels, and to different actors, can be perceived as a threat. The third section will review how previous literature has situated studies of disinformation in a European
context. The last section in this literature review will discuss and argue for the chosen theory’s relevance to the issue - the threat of digital disinformation within the EU.

2.1 Digital Disinformation as a Concept

The first part in this literature review will look at the term disinformation and how previous researchers have discussed and relates the term and concepts, such as fake news, from a theoretical viewpoint. As Armitage and Vaccari (2021) argue, the lack of a clear definitional consistency can conflict academic findings and influence researchers’ understandings of the issue, including its potential solution. Hence, it is necessary to gain a better understanding of the implicit meaning behind the concept of disinformation, when moving forward, as Armitage and Vaccari´s (2021) argument holds true in the case of disinformation and its related terms. To better the contextual understandings and identify the appropriate conceptualisation relevant for the research puzzle, a clear definition needs to be determined.

There is a consensus on the definitional term of disinformation in studies conducted on the various approaches adopted by the EU to fight or regulate the dissemination of disinformation. Several scholars have utilised the EU definition of the term which states that disinformation is “false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit” (cited in: Hedling, 2021, Durach et.al, 2020, Brites, et.al, 2022). Due to this thesis’s research focus on the EU, this will be the relevant conceptualisation adopted in the analysis of the EU’s policies on disinformation.

Elsa Hedling (2021) is one of the above-mentioned scholars who adopts the EU definition. However, she takes the definition further by adding the word “digital” to clarify that this is a new form of disinformation threat, which has brought new actors and thus needs a new response. She states that “[d]igital disinformation refers to the use of digital tools in the dissemination of disinformation” (Hedling, 2021:844) which today is closely linked to social media platforms. This is an important aspect to acknowledge since disinformation is in no regard a new phenomenon. On the contrary, it has existed in numerous forms throughout history. The term digital disinformation however points more directly at the contemporary issues societies face today with new actors entering the scene through social media platforms, as argued by Hedling (2021). As such, this contemporary definitional perspective will be taken and operationalized in this thesis, making Hedling´s work an important source moving forward.
From the empirical evidence found in Romanova et.al (2020), it is suggested that the EU adopts additional concepts such as fake news in their discourse. They argue that the choice of word is crucial as disinformation is a more neutral and broader term whereas fake news “exclude the possibility of an honest mistake” (2020:57). Armitage and Vaccari (2021) states that the term fake news is a simplification of the bigger issue, an argument which will be adopted in the line of thinking throughout this thesis. Additionally, they point to the fact that the term has been seized by politicians to disregard and deem unfavourably news statements or those who contradict their political view and agenda. Durach et.al adds to this by arguing for a more “inclusive and complex approach” which they argue the term disinformation brings in contrast to the term fake news. According to the authors, the term fake news is “inadequate, imprecise and misleading” (2020:6).

To summarise, this thesis will draw its conceptualisation from the EU’s definition of the term, utilised by several scholars, as well as Elsa Hedling’s (2021) more narrowed and contemporary addition of “digital disinformation”. How this term relates to (in)security more generally, and more specifically, how it can be perceived as a threat to the EU, will now be discussed.

2.2 Digital Disinformation as a Security Threat

The spread of digital disinformation and the conspiracy theories which it feeds has during the past few years surfaced in academic IR literature as a threat to mainly Western democracies. With a clearer definition of the term in mind, this section will now discuss the security aspect of this issue and how it is discussed in the relevant literature, significant for answering the research question of How has the EU’s perception of disinformation as a threat evolved/changed between 2018 and 2022?

As such, the first part of this section will focus on the concept of threat construction and perception within the EU.

When it comes to discussing the EU’s perception of threats one of the most important works, which this thesis utilises and draws upon is that of Christopher Baker-Bell and Gareth Mott (2022). While their research examines the EU’s perception of the threat of cyberterrorism, this thesis believes that their findings are relevant for this research as they offer a valuable framework for analysing how the EU constructs its threat perceptions. Primarily, Baker-Bell and Mott’s use of interpretive discourse analysis provides a compelling way to understand how the EU’s perceptions of threats are constructed and articulated. They argue that the EU’s
responsibilities in the field of security have expanded, allowing it to be viewed as a “holistic security actor” that addresses both internal and external security threats. They also note that the EU has broadened its scope to include more than the traditional issues of military and defence (Baker-Bell & Mott, 2022), thus taking a critical security studies approach. This can certainly be suggested for the case in today’s era of new technology and digital disinformation, which poses both an internal and external threat and calls for a non-military response. The complexity of this issue further calls for a multi-level and multi-actor approach which, when arguing in line with Baker-Bell and Mott, the expansion of the EU as a holistic security actor allows. This will be discussed further in the next section.

Furthermore, this relates to the form of consensus identified in the literature which states that the EU started to view disinformation as a potential threat after Russia’s annexation of Crimea in 2014. This was followed by Russia’s so-called “information war”, thus “the engagements against disinformation were led by an external threat perception” (Datzer & Lonardo, 2022:1). Again, this sequence of events points to how digital disinformation is a current issue facing the EU and not to other, less contemporary, forms of disinformation, i.e. not digital. It also emphasises that digital disinformation is a social threat, constructed by discourse and language in an abstract form.

In order to identify a possible shift in the EU’s threat perception, the different threats that disinformation pose to the organisation needs to be identified. The relevant literature has, as previously mentioned, been taking a critical security studies approach in that it includes more actors than simply the state and a broader notion of issues than simply armed conflicts. This next part will discuss the threats identified within the realm of critical security studies.

Several scholars have made the connection between populism and the spread of disinformation and conspiracy theories on social media platforms. This is central to the concept of disinformation and a crucial part of the EU’s vulnerability. Moreover, this is emphasised by Hedling (2021) who points to the complexity of EU policy making as a potential reason. Since few citizens understand it, a gap is created between the EU and its citizens, something Eurosceptic and populist movements have taken advantage of. Even if the word “populism” is frequently used in the literature, it is important to point out, in line with Tumber and Waisbord, that the term is a “notoriously ambiguous concept” (2021:16), and it entails a variety of political traditions and beliefs. The common denominator is nonetheless the promotion of themselves as the honest representation of “the people”. The thesis thus draws from this conceptualisation as it entails more than terms relating to political ideologies.
Wojczewski argues that these conspiracy theory spreading groups for long have been neglected in the IR literature, even though they have a focus which include classical IR aspects like the global power, influence and order (2021). It is therefore important not to neglect them in this thesis. These conspiracy theories feed on disinformation in particular on forms which construct a political “Other” as a corrupt and lying elite, typical of the political establishment. This type of discourse is fuelled with emotion driven language to invoke feelings of animosity and the will to act (Wojczewski, 2021).

At the centre of this issue of the regulation of disinformation lies a complicated system of competing interests and priorities. The most prominent one being the principles of free speech and the right to access information and the somewhat contradicting need to find regulation policies which promote public security. This is what Romanova et al refers to as the “paternalistic” and “adaptive” paradigms (2019). They can be “pictured at the opposite ends of a continuum, one extreme of which is public freedom [adaptive] and the other public security [paternalistic]” (Romanova, et.al, 2019: 55). This is additionally discussed by Matteo Monti (2021) who calls on the risks with a “privatization of censorship” and furthermore highlights the need to recognise the risks, together with benefits of regulating disinformation. In his analysis on the 2018 EU Code of Practise on Disinformation he argues that it is the attempts to regulate the dissemination of disinformation itself that can be seen as a form of threat, namely a threat against free speech and thus democracy (Monti, 2021). At the heart of this information dichotomy is the social media platforms, and the co called “platformatisation of news distribution” which has reduced “the role of Journalists as gatekeepers of news” (Monti, 2021: 214) which is “entailing both opportunities and threats” (Datzer & Lonardo, 2022:1). These private actors furthermore “have the potential to alter political processes by challenging traditional forms of political communication” (Datzer & Lonardo, 2022:1) in the way in which they promote their users to share their opinions. Nothhaft et.al. (2018) adds to this notion of public opinion and its importance for this security discussion. With a focus on Western democracies, they argue that opinion formation in these states is often characterised in ways which distinguishes them from non-Western democracies, such as a system of “free opinion formation”. These features, they argue, are great strengths for a society. However, they also create considerable vulnerabilities as it induces an environment in which disinformation easily can spread. Arguing against Monti and his view on the regulation of disinformation, they draw on Immanuel Kant and John Stuart Mill’s conception on what the word “free” actually entails and ask, “can there be a public interest in circulating statements that are factually wrong?” (Nothhaft et.al., 2018:30).
As previously stated, the issue of digital disinformation is not limited to domestic sources but also involves the perception of external threats. This relates to the interference of foreign states and governments, such as Russia, in matters that impact the democratic process such as elections. These external actors can engage in the dissemination of false information through various digital platforms, with the intent to influence public opinion and sway the outcome of important events. It can also extend to other democratic issues such as the creation of social unrest and instability (Romanova et. al., 2019, Datzer and Lonardo, 2022). This type of external threats started to receive mainstream attention after the Brexit referendum and US 2016 election as Russia was accused both times of so-called “information meddling” (Romanova et. al., 2019:54). Non-state actors such as Boko Haram, Al-Qaeda and the Islamic State in Iraq and Syria have also been pointed out as disinformation spreading actors and seen as a major security threat in their way of radicalising Western citizens (Hedling, 2021). This points to the diversity of disinformation and how it is everywhere at all points and thus making it hard to regulate.

2.3 A European Approach in the Fight Against Digital Disinformation

This part in the literature review will take a closer look at the EU and how the organisation has been tackling the issue of disinformation and different approaches taken by scholars to study it.

Scholars have employed a variety of approaches to study the issue of disinformation and its impact on European politics and society and among the approaches taken by the EU the multilevel and multi-actor approach has emerged as a particularly useful framework for understanding the complex dynamics at play. This approach is furthermore one that is favoured by scholars relevant to this thesis. In other words, it is widely believed that the EU can only effectively combat the spread of digital disinformation by ensuring the inclusion of all relevant actors across all levels of participation. Thus, a multifaceted approach is employed.

Belluati and Fubini (2022) argue in their article that the issue of disinformation requires a multilevel approach with multi-actor participation, entailing a focus on “fact-checking processes, the public actors and the policy lines to be adopted” (2022:59). The focus in their analysis is the approach taken by the EU, more specifically the European Digital Media Observatory (EDMO), which they argue to be “in institutional and procedural terms [...] the world’s most advanced to date” (2022:59). The conclusions drawn by the authors is that because of the methodical complexity of disinformation and its ability to reach and influence diverse communities with a range of different goals, the counter initiatives must thus be as complex
(Belluati & Fubini, 2022). Tumber and Waisbord state in agreement that the source of disinformation and the spread of it occur in three main levels: “individual, group, and systematic/structural” (2021:22) and in order to act against these threats societies and organisations needs to have a multipronged approach (2021). The approach taken by the EDMO does combine several levels and actors but has met some difficulties as member states and online platforms have been hesitant to follow the guidelines. The Covid-19 pandemic has however amplified the debate and made the need for a collective response more attractive (Belluati and Fubini, 2022). Likewise, Romanova et al has an inclusive approach in their study, conducted by analysing various EU documents from different EU institutions as well as the member state Lithuania. They conclude that there is a “lack of a single EU vision of how to ensure resilience to information threats” (2019:64). In other words, even though the EU as an organisation seems to have a multifaceted approach against disinformation, it is important to note that the approach may differ depending on the specific institution or member state that one is looking at.

There seems however to be some levels missing. Brites et.al (2022) has a generational focus in their study, arguing that the EU lacks a “generational-oriented approach” to be able to properly fight disinformation since different age groups receive and share disinformation differently.

Romanova et al (2019) place much emphasis on the importance of language in their study, highlighting the importance of linguistic analysis. This aspect will become important for this thesis as well. By utilising discourse analysis, Romanova et al analyse EU and Lithuania documents on the countering of disinformation and present the “plurality of the Union’s approaches to ensure resilience” (2019:53).

In conclusion, scholars advocate for a multifaceted approach when analysing the EU’s fight against digital disinformation as it involves multiple actors on multiple levels. This approach is deemed necessary, these scholars argue, due to the complex and multidimensional nature of the issue at hand, which has the potential to influence a range of actors. Actors range from individual social media users to entire nation-states, it is argued. Hence, as the EU is suggested to take this multifaceted approach it is important to understand the approach in order to situate the relevance of previous researchers’ findings in relation to this study.

2.4 Theoretical Perspective
The last part of this literature review will review the theoretical perspectives taken by previous researchers on the subject and argue for theoretical approach taken. As previously mentioned, digital disinformation is not a traditional security threat thus traditional IR theories (or grand theories), particularly realism and liberalism, have struggled to grasp the full effects of the technological revolution and the security issues which has followed. The main issue regarding these theories is that the few times when disinformation is discussed it is not seen as a valid security concern. This narrowness can be the reason of, for realists, the focus on material factors and international structure. Or with liberal theory, it is the focus on cooperation and integration which has led to the limited contribution in disinformation research (Eriksson & Giacomello, 2006). Indeed, when turning too schools where the social world is upheld over the material one, a more comprehensive theoretical approach can be found.

A large part of the above-mentioned scholars has a focus on the EU’s normative power and its identity which is something this thesis draws on. In relation to the EU as a normative power, a theoretical notion deemed relevant and adopted in this thesis with regard to previous research, the concept “securitization” becomes relevant to investigate closer moving forward in this section. However, in the first part of this section the thesis will describe the discussion on the EU’s normative power and identity.

Elsa Hedling follows a scholarly field of social theory which has focused on “how norms, roles and identities have shaped the practical enactment of EU foreign policy” (2021:842) and turns to international practice theory in her study. This theory puts an emphasis on how social practices, norms and beliefs shape and influence how actors behave in the international system. She argues that an “overlooked dimension of the change brought about the increasing need to counter digital disinformation is located in the everyday practice of those involved in that work” (Hedling, 2021:845).

In Brites et al’s article, the authors discuss the role of EU’s identity, stating that the organisation views itself “as a normative global power” and that “the EU sees itself as a promoter of universal norms and principles in its relations with non-members, but also within its own borders” (Brites, et.al, 2022:352). Democracy and human rights are a cornerstone in this identity and the promotion and protection of said values are essential to the EU’s aims and objectives. This type of identity can help and explain the growing concern within the organisation regarding the increasing spread of disinformation as it can pose a threat to democracy and undermine human rights, and thus EU’s identity as a normative global power. As such, the article argues, combating disinformation has grown to become a priority for the
EU and by developing measures to limit the dissemination of digital disinformation the organisation is able to protect its values and identity (Brites, et.al, 2022).

Moreover, it has been argued in the literature, as well as this literature review, that digital disinformation is a social threat. Hedling (2021) being one of the authors viewing disinformation as a social threat which is closely linked with the emergence of social media and the speed of digital information. Scholars like Datzer and Lonardo (2022) have discussed the perception of digital disinformation as a threat and this, the thesis argues, clearly points to the issue as a social threat. This because of its discursive nature and ability to influence societies on multiple levels in the way that it can, for instance, alter public opinion as well as harm the public health, as seen in the Covid-19 pandemic. Digital disinformation furthermore lacks specific time and place but is constant and universal. The literature review has also identified populist movements as a group who use disinformation to influence others. These groups are also heavily influenced by identity and norms in their form of “Othering” (Wojczewski, 2021).

As this thesis is focused on threats perception and (in)security of a transnational organisation, and security studies is a clear subpart of IR, the concept “securitization” is relevant to shine a light on and discuss more closely. However, it is important to note that disinformation is not often recognised as a threat in a traditional view. In other words, it is not a state threatening another state through anarchy and war, but it is an abstract concept, tainted by subjective interpretations. Hence, the threatened object is heavily influenced by norms and identity. The thesis therefore utilises and is guided by securitization theory, a critical security studies theory, in the form given by the Copenhagen School. Hedling’s international practice theory does thus fall short when it comes to viewing disinformation as an existential threat. While this theory emphasizes digital disinformation as a social practice, it does not fully capture the existential threat perception, urgency, and intensity that securitization theory provides. Securitization theory offers a more comprehensive understanding of disinformation’s potential impact, particularly in terms of existential threats, which is crucial for the focus of this research. Digital disinformation in the context of securitization theory can be framed as an existential threat to the EU’s core values, democratic institutions, and social cohesion. In contrast, international practice theory, particularly Hedling’s perspective, emphasises EU norms and normative influence (2021). However, it fails to integrate within the security framework and thus lacking an analysis of how disinformation can pose a threat to these norms and identity in a security context. Securitization theory, on the other hand, offers a more comprehensive framework. The theory explores the interconnections between norms, identity and security (Trithara, 2020). This enables the examination of digital disinformation and its impact.
on the EU’s democratic norms, societal identity and political security, all within the same theoretical framework. Securitization theory additionally has a constructivist framework which is apparent when reviewing the content which can provoke a “securitization move” (Trithara, 2020) and this framework is moreover helpful when analysing conflict and threat constructions.

Securitization theory covers the idea that security is a speech act which puts the attention on language and how it can implement action, in other words “the function of language” (Balzacq, 2011:4). Scholars of securitization theory argue that “security is about survival” (Buzan, et.al, 1998:2) meaning that when an actor presents an issue as an existential threat to a selected and specific object, it is about the survival of said object. A threat is existential when the known order, if not eliminated, ceases to exist which legitimises the use of force. The securitizing actor can implement emergency actions that otherwise would not be accepted under these conditions (Buzan, et. al, 1998: 23-24). This causes an issue to become securitized as a securitizing actor presents it as an existential threat to an audience, and the audience accepts it as such.

Dakoda Trithara has in her study on disinformation utilised securitization theory as a theoretical framework and states that:

“Securitization rests on the ability of an actor to identify issues to be treated as security threats, and focus on the process by which rhetorical moves allow actors to create a situation where extraordinary measures or other steps to deal with an existential threat to some referent object can be legitimized” (2020:2)

However, in relation to the EU, it is to some extent what constitutes its norms, identity as well as strengths, which is what also is threatening the organisation, i.e., democracy and free speech, as previously discussed by Nothhaft et.al. (2018). Furthermore, such a construction makes the EU vulnerable to both internal as well as external disinformation threats and as noted by Buzan “states can be just as thoroughly disrupted and destroyed by internal contradictions as they can by external forces” (cited in Trithara, 2020: 6). The fact that digital disinformation poses both an internal and external threat to the referent object has been evident in the previous sections, and it is viewed as an existential threat because of its ability to undermine democratic institutions. The Copenhagen School holds securitisation to be “an inter-subjective process as it is impossible to objectively determine if a threat is really a threat as different actors have various understandings and thresholds for what constitutes a threat” (Trithara, 2020:5). This is where the social construction can be seen.
The process of securitizing disinformation has previously been studied in different contexts however with a main focus on the unit level of analysis. This thesis will move beyond the unit level to also include the regional- and system-levels of analysis. Trithara’s study has a clear unit level focus namely a focus on securitization of disinformation in the UK after the Brexit referendum. The article analyses how the DCMS (Department for Digital, Culture, Media and Sport) has securitized disinformation. This was done by analysing the DCMS reports by identifying distinct speech acts which securitized disinformation. The study moreover assesses the responses form the intended audience, including the UK government and Facebook, to evaluate the effectiveness of the securitization process (Trithara, 2020).

A different example on a unit level study is Jackson’s study which through the theoretical lens of securitization analyses the Canadian government and their reaction to disinformation campaigns stemming from foreign actors (Jackson, 2021). These cases have a focus on disinformation as a tool used by foreign entities. However, these analyses primarily target the unit level in terms of their audience, not extending their scope to address disinformation at the system- or sub-system level, despite the external projection of the threat. In essence, while these studies highlight disinformation as a weapon employed by external actors, their focus remains predominantly on the specific units or entities affected, overlooking the broader systemic implications of the threat originating from external sources. This thesis goes beyond and will incorporate more than the unit level and delve into the broader regional or subsystem level, exploring how the EU as a regional actor has perceived disinformation as a threat. Additionally, the analysis extends to transnational actors, specifically social media and other tech companies, serving as the audience for the EU’s securitization efforts against disinformation. The initial referent object of the democratic processes and institutions and the security and integrity of information moreover have system level qualities. Buzan et al. emphasises that objects including international society and democracy can be viewed as being referent objects on the system level (Buzan et al., 1998: 38). By including more in this analysis than the unit level one can reach a more comprehensive understanding of the threat of disinformation. The emphasis on unit level analysis in studying the securitization of digital disinformation, or any other issues, stems from the observed challenges in achieving successful securitization on the system level, as demonstrated in Dewi’s (2020) research on the securitization of climate change. This does however indicate that there must be a successful securitization in order to be studied and be meaningful. Focusing solely on successful cases is biased as valuable insights and discussions can emerge from both failed and successful securitization attempts.
There has moreover been some criticism directed at the Copenhagen School for its state-centric notions of security. It is argued that the theory lacks a precise definition of the entities that can be classified as actors in the process of securitization. Trithara does however argue that the securitization actor must have authoritative power but does not need to be a nation state.

When it comes to what is being existentially threatened, i.e. the referent object, there can be several interconnected referent objects as discussed by Lene Hansen and Helen Nissenbaum in their article “Digital Disaster, Cyber Security, and the Copenhagen School” (2009). They furthermore argue that cyber security should be a “particular sector on the broader terrain of Security Studies” (Hansen & Nissenbaum, 2009:1157). The authors advocate for a framework that enables the recognition and examination of diverse discourses and the resulting disagreements within and beyond geographical and political confines. This highlights their theoretical framework which recognise the presence of multiple perspectives. And rather than identifying separate referent objects the authors conceptualise discourse as “constellations of connected referent objects” (Hansen & Nissenbaum, 2009:1171). This approach allows for a more comprehensive understanding of the dynamics of securitization and political processes within the field. This moreover relates to the linkage between the “network” and “individual” and “human collective” referent objects. Meaning that the idea is not that a private security discourse constructs the referent object to be the individual, but rather that the “individual” is connected to the referent object in societal and political contexts (Hansen & Nissenbaum, 2009). Hansen and Nissenbaum’s theoretical contribution enables a clearer combination of levels in studies on securitization processes and for this thesis as this holds true to the issue of digital disinformation, as a field in cyber security. While an individual may be the target of disinformation, its impact extends far beyond that individual alone. Thus, the referent object goes beyond the individual and the individual, or unit-level, security discourse is connected to political and societal referent objects on a regional- or system-level. This legitimises the EU discourse on regulating information online through securitizing it as a crucial threat to democracies. However, the same applies for communities advocating for free speech as they can challenge these regulatory measures. These are not two independent discourses with separate referent objects, but instead conflicting interpretations of the suitable relationship between individuals and the state within the framework of a liberal state. This approach can moreover add to the analysis of securitization at the regional/system level alone, considering the presence of multiple referent objects in such contexts.
3.0 Research Design

In this chapter of the thesis, the research design will be presented, i.e., the chosen methodology used to conduct the research. The purpose is to give a clear outline of the methods employed and argue for why they were deemed the most fitting for this thesis. This chapter is furthermore arguing for its chosen data and giving an overview of its meaning and purpose, as well as discuss how it will be analysed in line with the methodology in order to answer the research question.

3.1 What’s the ‘problem’ represented to be?

Given the theoretical notions of this thesis, presented above, the methodology will take an interpretive approach in light of the Copenhagen School’s view of threats as socially constructed. This is because the concepts and issues discussed, such as the EU’s perception of threats, are inherently social (Hedling, 2021) and thus not easily quantifiable through positivist notions of objective truth.

It is common to utilise some form of discourse analysis when studying threat perception (Baker-Bell & Mott, 2022, Trithara, 2020, Datzer and Lonardo, 2022) and this includes scholars of the Copenhagen School. To be more precise, scholars of the Copenhagen School only employ discourse analysis as a methodology to explore and examine the phenomenon of securitization and it is restricted to be in the forms of spoken or written contexts (Hansen & Nissenbaum, 2009). The field of discourse analysis is however broad and entails a variety of schools and it is surrounded by several debates. This is partially due to the difficulty of determining a clear definition of what discourse entails.

To answer the research question, this thesis will utilise Carol Bacchi’s “What’s the problem represented to be?” (WPR) approach. She describes discourse as “forms of social knowledge that make it difficult to speak outside the terms of reference they establish for thinking about people and social relations” (Bacchi, 2009:35). Thus, the primary emphasis of this approach lies not in how individuals construct arguments but rather on exploring the fundamental thought patterns that form the foundation of political practices. Bacchi further states that the concept of “knowledge” is not regarded as an established wisdom to be obtained. Instead, it is recognised as a product of ongoing political debates and disagreements. The primary concern does not revolve around seeking or generating knowledge but rather delving into the intricate connections between all types of knowledge and their relationship with matters
of power and politics. The focus lies in understanding how knowledge is shaped, influenced, and utilised as a means of exerting influence and control within various societal contexts (Bacchi, 2023).

The aim of the WPR approach is to uncover the underlying assumptions and power structures embedded in policy discourse. Considering the theoretical lens taken in this thesis, the EU as a normative power and securitization as “the ability of an actor to identify issues to be treated as security threats” (Trithara, 2020:2), the method can be suitable for identifying change in the perception of disinformation as a security threat within the chosen timeframe. The method is used to analyse how policy issues are framed and represented with the recognition that the way a problem is defined and presented in public discourse has significant implications for policy outcomes. At the core of the WPR approach lies the question “What is the problem represented to be?” Bacchi argues that policy issues are not objective and neutral, rather they are the products of constructed discourses that are shaped by political and social interests. By understanding how problems are represented in policy discourses, one can gain insights into the ideologies and power dynamics that underpin policy decisions (Bacchi, 2009).

The approach encompasses and is constructed around a series of six interconnected questions as a guide which can facilitate the analysis of specific policy problematizations. Since, “by their nature policies make change, implying that something needs to change. Hence, there are implied ´problems´” (Bacchi, 2009: 9). The questions are:

1) What’s the ‘problem’ represented to be in a specific policy or policy proposal?
2) What presuppositions or assumptions underpin this representation of the ‘problem’?
3) How has this representation of the ‘problem’ come about?
4) What is left unproblematic in this problem representation? Where are the silences? Can the ‘problem’ be thought about differently?
5) What effects are produced by this representation of the ‘problem’?
6) How/where has this representation of the ‘problem’ been produced, disseminated and defended? (Bacchi, 2009: 2)

The foundation of this methodology draws upon the blend of theoretical frameworks, of post-structuralism, feminism, social constructionism, and Foucault's concept of governmentality. These theories reflect a shift towards interpretative methods within the field of IR, prompting a heightened awareness of how discourse actively constructs and generates “problems” As a result, conventional “problem-solving” assumptions, which have been
prevalent in much of the literature, are being critically examined and brought into question. This has however faced criticism from several scholars within the field due to the absence of well-defined methodological procedures. Malte Riemann (2023) address this debate in his article regarding the WPR approach and argues that Bacchi’s approach “ameliorates many of the criticism directed against [interpretivist approaches] as it provides IR scholars with a robust, versatile and replicable […] methodology for policy analysis and the constitution of policy ‘problems’” (Riemann, 2023: 154).

Bacchi argues that this alternative perspective challenges the prevalent notion that policymakers are mere “problem solvers”, suggesting that the idea of “problems” existing independently of the policy-process, waiting to be resolved, is overly simplistic and needs to be reconsidered. In other words, “Policies are examined not from a problem-solving perspective, but from a problem-questioning perspective” (Riemann, 2023: 155).

The objective with Bacchi’s six questions (presented above) is to serve as practical tools and empirical indicators which are to be utilised and applied to the data. She does however point out that not all questions need to be included in the analysis but can be selected based on the specific objectives of the study (Bacchi, 2009). Since this thesis focuses on the securitization discourse on two specific occasions and the potential change between these two specific points in time, and not on how this problem representation came about or the outcome and impact of the securitization, question three, five and six will not be a part of the analysis as this thesis is not concerned with identifying neither the effects nor the conditions leading up to the initial discourse.

3.1.1 Question 1

The aim of the first question is to “identify implied problem representation in specific policies or policy proposals” (Bacchi, 2009:4). In other words, the foundation of the WPR approach is that all policies are “problematising activities” and therefore they consist of implied “problem representations”. Bacchi argues that “how you feel about something determines what you suggest doing about it” (2009:3). Thus, during policy analysis, the proposed or recommended solution provides insight into how policymakers perceive the nature of the problem. In the context of a single policy, it is a common occurrence to encounter numerous proposals and, as a result, several distinct representations of the underlying problem, due to the complex nature of policy issues. It is however important to mention that a policy can have more than one problem representation as discourses can be intertwined (Bacchi, 2009).
3.1.2 Question 2

Once the first question is answered “the real work begins” (Bacchi, 2009:5). The aim with question 2 is to “identify and analyse the conceptual logics that underpin specific problem representations” (Bacchi, 2009:5). “Conceptual logic” points to the essential meanings necessary for a specific problem representation to come together cohesively and be meaningful. In other words, the aim of the second question is to uncover the underlying reasoning behind the problem representation. It seeks to identify the assumptions and presuppositions that are taken for granted, as well as any potential aspects that could have been questioned. By doing so the question functions as an important tool for identifying the background knowledge that underpin the problem representation, i.e. the assumptions (Bacchi, 2009).

Bacchi introduces an analytical approach to uncover the assumptions within the problem representation. This approach involves examining the “key concepts” present in policy texts, as these texts can be interpreted to reveal underlying political ideas. Additionally, Bacchi suggests utilising “binaries”, which consist of an “A/not A” relationship, to further analyse policies. By doing so, the prevailing idea or value is brought to the forefront, shedding light on its significance (Bacchi, 2009).

3.1.3 Question 4

The objective of question 4 (What is left unproblematic in this problem representation? Where are the silences? Can the ‘problem’ be thought about differently?) is to bring attention to the issues and perspectives that have been marginalised or overlooked in identified problem representations. By posing this question, the goal is to highlight aspects that might have been silenced or ignored in the process of defining and framing the problem. Bacchi advocates for the same techniques as for question 2 in order to identify issues that may have been silenced (2009).

3.2 Operationalization

Due to the qualitative nature of this research, it is important to present clear operational definitions. The theoretical notion of this thesis draws on the literature in the field of critical security studies and as previously mentioned, utilises the theoretical framework of
securitization theory in combination with the analytical tools of Bacchi’s WPR approach to answer the posed research question of *How has the EU’s perception of disinformation as a threat evolved between 2018 and 2022?*

The discourse analysis advocated by Bacchi is a crucial tool to uncover hidden meanings and latent assumptions in the EU’s Codes of Practice. Moreover, this analysis will bring to light the key discourses present in the material, which will subsequently undergo a deeper examination through the perspective of securitization theory. In order to identify said assumptions and more the question discussed above will be applied, i.e.:

1. What’s the ‘problem’ represented to be?
2. What presuppositions or assumptions underpin this representation of the ‘problem’?
3. What is left unproblematic in this problem representation? Where are the silences? Can the ‘problem’ be thought about differently?

For the purpose of this thesis the WPR approach and securitization theory play two important roles as the two approaches complement each other. Securitization theory provides insight into how the EU as an actor securitize disinformation by emphasizing the process of framing disinformation as a security threat. It identifies who the key securitizing actors are, their motives and referent objects, and how this influences the perception of disinformation as a threat. The WPR approach additionally focuses on policy representation, language choices and the broader political context. The approach moreover provides a framework to explore how disinformation is represented in policy documents, which helps to understand the evolution of policy responses over time. By combining securitization and WPR securitization theory helps to identify the securitization moves made by actors, while WPR analyses the policy representations. Comparing these elements between the two Codes of Conducts on Disinformation enables the thesis to identify shifts in securitization moves, changes in policy and language, and evolving threat perceptions within the EU. The distinction between actors and policy is crucial. Securitization theory leads to the understanding of why specific actors perceive disinformation as a threat while WPR sheds light on how these perceptions are translated into policy responses. The integration of these perspectives provides a comprehensive understanding of the EU’s evolving threat perception on disinformation, considering both the actors driving the securitization process and the policies that result from it.
3.3 The Data

The data utilised in this thesis has been sourced from reliable and verifiable EU official documents, these documents are openly accessible to the public and can be found on EU websites. Furthermore, the EU has a reputation for high standards of transparency and accessibility, which has made it possible to obtain the necessary information required for this thesis. Thus, it can be argued that the data used in this thesis is valid and derived from trustworthy sources that are readily accessible to anyone seeking information on the EU.

The data consist of the EU “2018 Code of Practice on Disinformation” in combination with the “2022 Strengthened Code of Practice on Disinformation”. This data emphasises the relationship with social media platforms, and other forms of tech companies, with the dissemination of digital disinformation. The Codes were first of its kind where the social media industry on a voluntary basis agreed to terms of self-regulation in order to reduce the spread of disinformation (European Commission, 2022). These Codes are with other worlds a soft law instrument which suggests, to those who sign, strategies they should adapt to regulate their platforms (Monti, 2021). The 2022 Strengthened Code of Practice is moreover an extension of the 2018 Code with the aim to set a “more ambitious commitments and measures aimed at countering online disinformation” (European Commission, 2022). The Code of Practice, both from 2018 and 2022 aim to combat the spread and impact of disinformation on online platforms. It was first developed, and later elaborated, in response to growing concerns about the negative effects of disinformation on democratic societies, such as its ability to undermine public trust, interfere with elections, and incite hate and violence (European Commission, 2022).

These two Codes are not the only policies against disinformation which the EU has produced. In fact, several other initiatives have been taken in the fight against digital disinformation including the Action Plan on Disinformation, the European Democracy Action Plan and the European Digital Media Observatory. However, the two codes are chosen and deemed important for the purpose of this thesis, which seeks to analyse whether there has been a noticeable shift in the EU’s perception of digital disinformation as a threat to its security. The reason being that both codes have a shared objective of addressing the problem of disinformation, with one Code being the addition of the other, unlike the other initiatives. This makes it easier to detect any change in language and framing to address its security concerns. Given their central role in the EU’s collective efforts to combat disinformation, the Codes represent a significant source of data. The WPR approach has an emphasis on policy and when applied to the analysis of the two versions of the Codes of Conduct it enables a detailed
examination of policy transformation. The strength of WPR lies in its ability to facilitate comparative analysis (Bacchi, 2009), making it particularly effective for understanding the changes evident in policy documents like the two Codes of Conduct.

Scholars have previously analysed the EU Code of Practice on Disinformation assessing its effectiveness and issues (Monti, 2021). In this thesis however, the focus will remain on a possible shift in framing and language rather than assessing its impact.

3.4 Limitations and Potential Biases

In this section the thesis discusses the potential limitations and biases that may be presented in the conducted research as well as the relevant arguments which will provide validity to the research.

A potential issue is the limited scope of the data. This might affect the analysis as the documents used for the research may not yield a complete view of the EU’s possible shift in its overall perception of digital disinformation as a threat. The thesis however argues that the data used is still sufficient and reliable as a source for its study. Firstly, since it is a central part of the EU’s campaign to limit the spread of disinformation it arguably represents the EU’s position on the issue of digital disinformation and can thus be seen as a primary source. Secondly, the documents discussed have developed through a process which reflects several EU institutions, such as the European Commission and the European Parliament (European Commission, 2022). The data can thus be argued to represent the EU as a whole and provide important insights, even if it can’t represent the whole of EU, its institutions and members.

4.0 Analysis

In the following chapter, the thesis will present its findings. These findings have been formulated through the methodological lens of the three questions formulated by Carol Bacchi. Moreover, the thesis has analysed the threat constructions encapsulated within the two versions of the Codes of Practice. This analysis will be closely aligned with the foundational tenets of securitization theory as discussed in the earlier chapters and thereby conduct an examination of the two Codes alignment with the core concepts of this theoretical framework.

4.1 what’s the problem represented to be?
The two Codes are directed at social media companies and other tech companies. This indicates that the EU views these entities as central players in the context of the dissemination of digital disinformation. The Codes places the responsibility for bringing about necessary changes squarely on the shoulders of these companies, suggesting that they are perceived as the problem that needs to be addressed. They furthermore assign them the responsibility for implementing essential reforms. The Codes was produced not to long after Brexit where the data company Cambridge Analytica has been accused to interfere, as well as the 2016 US election. The initial Code can be seen as an answer to these events where social media and other tech companies played a pivotal role in the dissemination of digital disinformation. During this time the perception of disinformation as a threat shifted from being solely attributed to foreign actors like Russia and their “information war” (Datzer & Lonardo, 2022) to expanded to include a broader concern, specifically addressing the middleman: social media platforms. These platforms were recognised as potential sources of disinformation, even without direct foreign interference. Consequently, the Codes of Conduct were aimed at regulating these intermediary companies. The codes do however go into more specific problem representations and the thesis will now discuss the ones relevant for answering the research question of: how has the EU’s perception of disinformation as a threat evolved/changed between 2018 and 2022? The focus will thus be on the differences in the two Codes regarding its problem representation.

4.1.1 Security of Ad Placement, Political Advertising and Issue-Based Advertising

Within the context of advertisements, the problem (i.e., what the Code wants to fix) in the 2018 case is argued to be the commercial aspect of advertisement and the promotion of accounts and websites which spread misrepresented and misleading information regarding themselves. One of the core ramifications of this problem is the erosion of trust among users, the distorting public discourse and making it increasingly difficult for them to differentiate between genuine and deceptive content. Regarding political and issue-based advertisement. The problem is the inconspicuous nature of political advertisements stemming from the lack of clear and explicit identification, making it difficult for users to discern between regular content and sponsored political messages. Therefore, individuals may unknowingly encounter and engage with political advertisements, unaware of their persuasive intent or the entities behind them.

The strengthened Code finds the scrutiny of ad placements an important aspect in fighting the spread of disinformation and the problem representation regarding ad placements.
revolves around the funding and monetization of disinformation. It highlights the urgency to prevent the financial support and promotion of false or misleading information through advertising systems. The problem is represented as a need to enhance policies and systems that regulate content eligibility for monetization and ensure accuracy and effectiveness in controlling ad placements to regulate and hinder the spread of disinformation. The Code moreover wants its Signatories to commit to stop the misuse of advertising systems to spread disinformation by strengthening cooperation between themselves. The problem representation here is the lack of cooperation in regard to how advertisements are used in the dissemination of disinformation.

The problem regarding political advertisement lies in its potential to go unnoticed and blend seamlessly with regular content, making it challenging for users to distinguish between paid-for political ads and organic posts or information. As well as the issue of not having a shared definition, making it difficult to regulate across the platforms. Additionally, the problem representation highlights the need for transparency in political and issue advertising.

This problem representation illustrates a shift in the EU’s threat perception as well as the securitization process. The 2018 Code has a primary focus on the political and commercial forms of advertisement. It emphasises the erosion of trust and the distortion of public discourse. At the unit level disinformation was securitized as it threatens the social fabric and democratic norms, and it was framed as mainly a commercial and political threat. However, in 2022 the securitization process deepens as the problem representation expands to include issues such as funding and monetization in its framing of disinformation. This system level approach frames the financial support and promotion of disinformation through advertising systems as a significant threat. The issue of advertisement is moreover closely linked to elections as it may interfere in public opinion and discourse. Here we can see a securitization on all levels of analysis as the issue of elections have an impact on the system level, as mentioned by Buzan et. al (1998: 38-39) when democracy is the referent object the securitization is systemic. It moreover reaches down to the unit level and individual who votes. The shift from political and commercial concerns to also include more system level issues reflects an evolution in the securitization process. The recognition of the need for shared definitions and cooperation as well as a transparency on the regional level demonstrated an understanding of digital disinformation as a multifaced threat in need of collective action, as discussed by Hedling, (2021), Durach et.al, (2020), Brites, et.al, (2022). This problem representation thus reflects a nuanced perception of disinformation including both its impact on the individual as well as on the regional and system level implications for democratic societies. This was evident in Hansen
and Nissenbaum article. They argued that rather than identifying separate referent objects the authors conceptualise discourse as “constellations of connected referent objects” (Hansen & Nissenbaum, 2009:1171). This approach allows for a more comprehensive understanding of the dynamics of securitization and political processes within the field. This moreover relates to the linkage between the “network” and “individual” and “human collective” referent objects as is evident in this problem representation. Meaning that the idea is not that a private security discourse constructs the referent object to be the individual, but rather that the “individual” is connected to the referent object in societal and political contexts (Hansen & Nissenbaum, 2009).

4.1.2 Integrity of Services

Regarding the integrity of services, the Code from 2018 states that the Signatories must commit to “put in place clear policies regarding identity and the misuse of automated bots on their services” (European Commission, 2018:6). The problem in this commitment is considered to be the spread of disinformation through the deceptive use of fake accounts and automated bots. The disinformation that fake accounts and bots generate poses a significant threat to the integrity of online platforms and the information shared within them in this problem representation.

In the Strengthened version form 2022 the issue of “integrity of services” relates to the commitment to “limit impermissible manipulative behaviours and practices across their services” (European Commission, 2022: 15). This concerns technologies or accounts which generate disinformation including foreign interference, artificial intelligence (AI), fake accounts and bots, hack-and-leak operations, impersonations, malicious deep fakes, the purchase of fake engagements and non-transpired paid messages or promotion by influencers. The problem is thus the ability and opportunity that these groups and technologies have to spread disinformation.

The problem representation suggests that addressing these manipulative behaviours and practices is crucial for combating the spread of disinformation effectively. By identifying and acknowledging these issues, the Code aims to encourage its Signatories to implement measures that increase transparency, accountability, and security in the digital environment.

In this problem representation, the 2018 Code demonstrates the initial securitization move by highlighting distinct threats such as fake accounts and bots. The 2022 Code points to a securitization process in motion by emphasising a broader spectrum of devious behaviours and
technologies as existential threats. The understanding of threats expands over time, which demands comprehensive policies to address the multifaced challenges posed by disinformation. This is moreover made more evident when analysing the different levels of securitization as all levels are interconnected in this case of disinformation. The unit-level of this problem representation emphasises the individual platforms and services. The Code from 2018 had a focus on specific issues like fake accounts and bots, reflecting a localized understanding of the problem. In 2022 the problem representation expanded to include different disinformation tactics such as deep fakes and hack and leak operations. This points to deeper concern from the integrity of individual platforms and to an expanded securitization move at the unit level.

Moving up to the regional level and the EU as a collective entity. The 2018 Code put emphasis on the need for policies to fight disinformation which indicates to a regional securitization move by the securitizing actor, in this case is the European Commission. By 2022 however the problem representation depends to also include issues such as foreign interference and other regional challenges. This threat development indicates a regional securitization process where the regional and collective understanding of disinformation as a threat became more prevalent. This further acknowledges the nature of disinformation campaigns for its lack of time and place and cross-border ability. This ties into what Baker-Bell and Mott discussed in their article and further strengthens their argument regarding the EU as a security actor. They argue that the EU’s responsibilities in the field of security have expanded, allowing it to be viewed as a “holistic security actor” that addresses both internal and external security threats, which has been evident in the problem representation. They also note that the EU has broadened its scope to include more than the traditional issues of military and defence (Baker-Bell & Mott, 2022). This reveals an evolution from localized concern to a more comprehensive view of digital disinformation as a multi-level threat which is moving beyond the military and solely political sector of security.

The level of the global digital ecosystem i.e. the system level of securitization is also evident in the Codes. In both 2018 and 2022 the problem representation recognized the global threats which disinformation pose. In 2018 the focus on bots and fake accounts indicated to a growing securitization process at the system level by recognising the potential global impact which digital disinformation can have. The 2022 Code again showed to become more comprehensive in its problem representation. It included advanced technologies like AI and influencer-driven disinformation campaigns and acknowledged its global scope. This broader inclusion suggests a more advanced securitizing move at the system level threat which requires coordinated efforts beyond regional boundaries.
4.1.3 Empowering Consumer and the Research Community

In the 2018 Code the commitment calls on the Signatories to invest in “technological means to prioritise relevant, authentic and authoritative information where appropriate in search, feeds, or other automatically ranked distribution channels” (European Commission, 2018:7). In today’s digital age, the spread of online content and the rapid dissemination of information across various platforms have resulted in an overwhelming volume of data where disinformation easily can be masqueraded as legitimate facts. The problem is thus the difficulty faced by consumers and the research community in distinguishing disinformation from factual information due to the limitations of existing technologies.

The Signatories furthermore commit to “support good faith independent efforts to track Disinformation and understand its impact, including the independent network of fact checkers facilitated by the European Commission” (European Commission, 2018:8). Hence, there exists a lacking knowledge of what digital disinformation entails as well as its impact.

In 2022 the problem representation is again the invisibility of disinformation and that EU citizens on online platforms lack the tools to identify it. Additionally, said users lack the media literacy and critical thinking to be able to identify disinformation, especially the more vulnerable groups. The Code moreover calls on the Signatories to provide the tools “to assess the trustworthiness of information sources, such as indicators of trustworthiness for informed online navigation, particularly relating to societal issues or debates of general interest (European Commission, 2022:23). This points to how “social issues or debates of general interest” are threatened by disinformation. The problem representation moreover highlights the importance of fact-checking in countering disinformation effectively. Fact-checkers play a crucial role in verifying the accuracy of information, identifying false or misleading content, and providing users with reliable and trustworthy information.

The evolution from the 2018 Code to the 2022 Strengthening Code in this problem representation reflect a shift in understanding disinformation as a threat. In 2018 the focus was primary on addressing technological limitations, emphasising the impact of disinformation at the unit level. Specifically, it is concerning individual users and consumers as well as the research community. The threat perception was rooted in the need to prioritize authentic information for said users. In contrast, the 2022 Code represents a broader and more nuanced understanding of digital disinformation as a threat. It again acknowledges the invisibly nature of disinformation and the lack of media literacy among EU citizens at the unit level. However,
the Strengthening Code continues its focus beyond the individual user and the unit at large. It highlights the social impact of disinformation on public debates and social issues of general interest which indicates a shift from a unit to a regional or system-level of securitization.

Between the formulation of the 2018 Code and subsequent Code from 2022, a critical event occurred which had an influence on the EU’s threat perception: the outbreak of the Covid-19 pandemic. This global health crisis transformed the media landscape and the dissemination of disinformation, amplifying its impact on public health and public discourse. This led to a heightened distrust in experts and institutions (Belluati and Fubini, 2022). This event can be seen as a reason to why we see this shift between the two Codes as, consequently, the EU’s understanding of digital disinformation evolved. This matured securitization process for the EU as an actor can be argued to have resulted in policy changes of the 2022 Strengthened Code. This updated framework not only recognise the impact of digital disinformation on individual users but moreover highlights the importance of addressing its broader societal implications. The EU’s response to disinformation in the 2022 Code became more comprehensive including not only a protection of public health and discourse but also a climate of trust in expert knowledge.

4.2 Assumptions and Prepositions

The assumptions and prepositions in the two Codes are closely linked to the key concept of technologically cantered solutions in the problem representations. However, there are some changes in between the Codes which indicates a shift in the EU’s perception on digital disinformation regarding its assumptions.

The EU relies primary on technological interventions and regulations aimed at social media and tech companies in the Codes to tackle disinformation online. By emphasising this tech focused approach and by addressing the social media and tech companies as the problem, the EU has assumptions which indicates a view which states the by implementing technological measures disinformation can effectively be combated. The underlying assumption in these perspectives is that regulating technology and algorithms holds the key to managing human behaviour and minimizing disinformation. The belief is that regulations can establish a controlled environment where the spread of disinformation can be contained. However, this approach, primarily focused on technological solutions, overlooks the fundamental issue of human behaviour that drives disinformation. The assumption inherent in these strategies is that
by gaining control over algorithms, disinformation can be mitigated, even though the root causes, which lie in human behaviours, remain unaddressed.

This assumption is seemingly rooted in events and the technological inventions at the time of the development of the Code and its Strengthened version. As previously mentioned, there has been reports of digital disinformation spreading on social media platforms in connection to elections and other democratic processes. Russia has additionally been accused of spreading disinformation on social media to influence foreign election in their so-called “information war” (Datzer & Lonardo, 2022). Hedling (2021) also mentions how non-state actors like ISIS, Boko Haram and Al-Qaeda have been pointed out as disinformation spreading actors and seen as a major security threat in their way of radicalising Western citizens online. The list grows long of examples, and it is not strange that this assumption permeates the Codes however at the opposite end of this approach lies the aspect of human behaviour, belief and biases. The assumptions framing this approach has a tendency to disregard the sociological dimensions of digital disinformation. As Wojczewski (2021) argues, disinformation is often fuelled with emotion driven language to invoke feelings of animosity and the will to act and exploits cognitive biases and emotional triggers. This aspect moreover puts emphasise on that digital disinformation is a social threat derived from discourse.

In the context of this assumption the EU’s perception on disinformation has evolved which is evident in the problem representations. In the first Code from 2018 the emphasise was largely on the technological means as well as addressing its limitations. The Code framed disinformation as a threat mainly on the unit level of securitization with a focus on individual users and their interaction with technological aspects which enabled the spread of disinformation. The Strengthen Code form 2022 still incorporate these aspects of technological solutions in disinformation dissemination while also relating the issue more to societal aspect and general debates.

The 2022 Code seems to follow the arguments of previous studies on the EU and its fight against digital disinformation which stated that the organisation is in need for a multi-level and multi-actor approach. The securitization process has evolved to a more comprehensive perspective which suggest that the EU’s treat perception has done the same. It includes a deeper understanding of disinformation with the incorporations of societal vulnerabilities and as a multifaced problem that requires more than merely technological solutions. There is also a shift from the unit level of individual users to a regional level of social norms and behaviour, revealing a more holistic approach. As an issue situated in the field of cyber security it is here
evident that there exists multiple perspectives and discourses and the referent objects are intertwined entities, as discussed by Hansen and Nissenbaum (2009).

4.3 What is left unproblematic in this problem representation? Where are the silences?

Moving on the last question which aims to uncover what is missing from the problem representation and what is left unproblematic. This section will again combine the analysis of the two Codes in order to more easily detect a change in the threat perception of the EU as an actor and if this becomes visibly in what is silenced in the organisations policies.

The central problem representation, clearly evident in both Codes, states that the problem which the Codes are to combat is the social media and tech companies which enables the spread of digital disinformation. This problem representation leaves somethings unproblematic in both Codes which in this context of silences are relatively similar in 2018 as well as 2022. It relates to other social media platforms or tech companies, which are not included as Signatories of the Codes, that targets disinformation and conspiracy spreading group. The Codes does not discuss the possibility or likelihood that individuals and groups will move to other platforms where the dissemination of digital disinformation is more prevalent. The Codes also overlook the potential for their existence to indirectly amplify the spread of digital disinformation within the problem representation. Wojczewski (2021) argues that the nature of groups who often spread disinformation online, i.e. different forms of populist groups and conspiracy theorists, is the “us against them” narrative. They feed on disinformation in particular in the form which construct a political “Other” as a corrupt and lying elite, typical of the political establishment (Wojczewski, 2021). In a constant evolving digital landscape individuals and groups can constantly move their disinformation onto other platforms. The reaction to the Code can mean just that, as these policies can be argued to violate human rights by the “controlling elite”, since they indirect control what people can and cannot say. Instead of solving the problem, will the Codes only move disinformation somewhere else? Hedling (2021) is another author who discuss these, often populist, groups and states that they are a crucial part of the EU’s vulnerability as these groups portrays the EU as the lying elite and themselves as the truth bearers for the people. In addition, Hedling argues that the complexity of the EU is taken advantage of to spread digital disinformation. This aspect of the complex issue that is the spread of disinformation is left unproblematic in this problem representation and does not evolve or change from 2018 to 2022.
This ties into the binary of upholding human rights/violating human rights discussed in the literature review. In the other problem representations, it was clearly stated that any efforts to address and regulate digital disinformation must take into consideration the fragile balance of the freedom of expression and not unjustly remove or restrict lawful content. It states: “[t]he Code shall apply within the framework of existing laws of the EU and its Member States and must not be construed in any way as replacing or interpreting the existing legal framework” (European Commission, 2018:2). The Code moreover follows the line that fundamental rights such as freedom of expression, freedom of information and privacy are important and needs to be respected. The need to balance the protection of said rights with taking actions against the spread of disinformation is acknowledged as well. The Code does however leave some aspects regarding this unproblematic. The text does not explore the potential tensions between freedom of expression and countering digital disinformation. It is thus a silence in the problem representations regarding how the Code and its commitments may restrict these rights in their fight against disinformation. This indicates that the EU as an actor is aware of the human rights implications the Code might have but chose not to go into it. This is what Romanova et al refers to as the “paternalistic” and “adaptive” paradigms (2019). The regulation of the spread of digital disinformation can be “pictured at the opposite ends of a continuum, one extreme of which is public freedom [adaptive] and the other public security [paternalistic]” (Romanova, et.al, 2019:55). The silence in the problem representations could be attributed to the EU’s concern about preserving its legitimacy and avoiding potential backlash from the audience. Explicitly stating that the Codes might restrict freedom of speech for citizens would lead to resistance and rejection of the policies. Trithara (2020) discusses that an actor must have authoritative power to successfully securitize an issue as an existential threat, which would evitable be lost if the actor where to go against its own norms and laws. In this context, attempts at securitizing disinformation could be perceived as unsuccessful, resulting in a cautious approach to framing the issue in the problem representations. This silence reflects a delicate balance between addressing the threat of disinformation and upholding democratic values and individual freedoms, highlighting the complexities involved in securitizing digital threats effectively.

This perspective somewhat aligns with Monti’s (2021) argument, that the true threat to democracies lies in the regulation of disinformation. However, rather than focusing solely on determining who’s right or wrong, the analysis emphasis an adoption of the framework advocated by Hansen and Nissenbaum (2009). This approach encourages the recognition and exploration of diverse discourses and disagreements within and beyond political and geographical confinements. As discussed above, their theoretical framework recognises the
presence of multiple perspectives, conceptualizing discourse as interconnected referent objects rather than isolated entities. In line with this approach, the adaptive and paternalistic paradigm and nature of the discourse should not be viewed as two independent discourses with distinct referent objects. Instead, they represent conflicting interpretations of the appropriate relationship between individuals and the state. This analysis underscores the plurality of referent objects and the interconnections between the network, the individual, and the human collective, illustrating the interconnectedness of various levels of analysis, from the unit up to the system level.

In examining the differences between the two Codes, it becomes apparent that the evolution of the EU’s perception of disinformation is rather limited in the context of this question. Both Codes address similar issues, and there is a notable absence of any clear effort to bridge the gap or fill the silence identified. If anything, the silence appears to have grown louder, especially considering the diminished mention of human rights concerns in the second Code. This amplification of silence might be attributed to the EU’s heightened perception of disinformation as a significant threat, possibly leading them to overlook certain core values in the organisation’s pursuit of combating it. After the implementation of the first Code, there were no indications of the potential migration of disinformation to other platforms. The Codes do not seem to have considered this possibility, assuming their success would prevent such a shift. Lastly, neither of the Codes has a generational focus discussed by Brites et.al (2022). They argue that the EU lacks a “generational-oriented approach” to be able to properly fight disinformation since different age groups receive and share disinformation differently.

5.0 Conclusion

The issue of digital disinformation has taken the world by storm in the last few years as both an internal and external threat to societies and, mainly Western, democracies. Several issues do however surface when trying to regulate the dissemination of digital disinformation, the most prominent one being the principles of free speech and the right to access information. Some scholars have argued that it is not worth the risk of limiting information (Monti, 2021), whereas others have stated that disinformation is a serious threat to democracies and needs to be regulated (Datzer & Lonardo, 2022). New initiatives are nonetheless continually made to try and regulate this new form of security threat and the EU is a prime example of this. The focus of this thesis has been to gain a deeper understanding of digital disinformation and the
security discourse which is surrounding the issue, more precisely, the construction and perception of disinformation as a security threat. However, in today’s digital world disinformation is rapidly evolving with the creation of new technologies and opportunities. The aim of this thesis has thus been to investigate if this has led to a shift in the perception of digital disinformation as a threat and therefore a change in the EU’s approach to combat the issue. This has been done with the toolkits from the methodological framework of Carol Bacchi’s WPR approach, in combination with the Copenhagen School’s theory of securitization. These frameworks have moreover been applied to the EU’s Code of Practise on Disinformation from 2018 and the Strengthened version from 2022. In light of this, the research question which is to be answered is:

*How has the EU’s perception of disinformation as a threat evolved/changed between 2018 and 2022?*

Securitization theory presupposes that certain issues can be framed and presented as security threats, demanding extraordinary measures or actions to address them. In the case of the two Codes of Practice the securitizing actor, which is identified to be the European Commission in both Codes, is identifying and characterising digital disinformation as a significant security concern. The overall findings moreover confirm that the EU is deepening its recognition of digital disinformation as a security threat. This is manifesting itself through the comprehensive and various ways in which it can harm information security, and thus democratic processes. For instance, the Code from 2018 is primarily focused on the erosion of public trust and democratic processes. This is shown by the focus on how disinformation can influence elections and public debates as well as potentially worsen societal divisions and tensions. The Code from 2022 on the other hand presents a broader understanding of the complexity of disinformation and the multifaced threat which it poses. This is due to its inclusion of issues such as the foreign interference and manipulative behaviour in the form of AI and deep fakes as well the funding and monetization of disinformation. This evolution points to an awareness of the evolving tactics and threats posed by digital disinformation. This is moreover a shift from the unit level of the member states and its individual citizens to a more regional level focus whit issues such as foreign interference. It is an evolvement of the securitization of disinformation made by the EU and the securitizing actors.

The expansion of the problem representations suggests that the EU’s perception of digital disinformation has evolved to embrace a more comprehensive understanding of the
multifaceted and complex nature of the threat which digital disinformation poses. This aspect goes in line with what was discussed by scholars in the field (such as: Belluati & Fubini, 2022, Tumber & Waisbord, 2021) regarding the multifaceted nature of digital disinformation. And the consensus that to combat this complex threat a multi-level, multi-actor approach is needed in order to be successful. This matured securitization process for the EU as an actor can be argued to have resulted in policy changes of the 2022 Strengthened Code. The analysis underscores the necessity of adopting a multifaceted approach in cybersecurity examination, emphasising the integration of diverse analytical levels. In doing so, it becomes evident that the theoretical concepts proposed by Hansen and Nissenbaum (2009) hold significant importance as incorporating their frameworks enriches the understanding of cybersecurity complexities.

Bibliography


