INSTITUTO
UNIVERSITÁRIO
DE LISBOA

The balance between effectiveness and proportionality in responding to Online Disinformation at crossroads: An analysis of the response of the European Union through security governance, 2015-2022

Sofia Cristina Martins Geraldes

Doutoramento em História, Estudos de Segurança e Defesa

Orientadores:
Doutor Bruno Cardoso Reis, Professor Auxiliar, ISCTE
Doutor Benjamin Farrand, Professor in Law & Emerging Technologies, Newcastle University

Lisboa, Dezembro, 2022

SOCIOLOGIA
E POLÍTICAS PÚBLICAS

Departamento de História

The balance between effectiveness and proportionality in responding to Online Disinformation at crossroads: An analysis of the response of the European Union through security governance, 2015-2022

Sofia Cristina Martins Geraldes

Doutoramento em História, Estudos de Segurança e Defesa

Orientadores:
Doutor Bruno Cardoso Reis, Professor Auxiliar, ISCTE
Doutor Benjamin Farrand, Professor in Law & Emerging Technologies, Newcastle University

Lisboa, Dezembro, 2022

Dedicated to my beloved husband

Acknowledgments

Doing a PhD and in particular writing a PhD thesis is one of the most challenging tasks. It challenges us physically, but especially mentally and emotionally, mostly because it is a very lonely journey. Nevertheless, this journey would be much harder without support, hence I dedicate these words to the people that made this path easier.

Firstly, I would like to give thanks to FCT - Fundação para a Ciência e a Tecnologia, this research project was conducted with the support of a doctoral grant awarded by FCT with the reference SFRH/BD/140797/2018. I would also like to give thanks to my supervisors Prof. Bruno Cardoso Reis and Prof. Benjamin Farrand, whose personal and academic support were fundamental to conduct this research and to write this thesis.

Secondly, I would like to give thanks to my beloved husband for his incredible support, this journey has been hard, but without his support it would be incredibly harder. I thank him for inspiring me, for always believing in me, for letting me know that and for supporting me every single day and specially on those days that was about to give up. I would also like to give thanks to my family, those who are physically here and to those who will always be remembered in my heart. In particular I would like to thank my grandma, who passed away during this journey, she will always be an inspiration of a woman way ahead of her time. I would also would like to give thanks to my friends.

Thirdly, I would like to give thanks to myself, for not giving in in the disinformation constantly spreading in my head, that I was not good enough and capable of achieving this goal of finishing my PhD thesis and my doctorate degree. Fortunately, I detected, I analysed and exposed that disinformation and I was able to improve my own strategic communication and overcome the challenge of writing a PhD thesis. Therefore, I would also like to dedicate this thesis to all academics around the world and especially to PhD students who struggle with this lonely journey, may they identify the way to improve their strategic communication and find the best strategy to fight their own internal disinformation.

Resumo

Este estudo analisa a consideração do princípio de proporcionalidade na resposta da União Europeia à desinformação online como ameaça à segurança. O uso da desinformação na política não é uma novidade. Contudo, o contexto político, económico, social e sobretudo o contexto tecnológico têm contribuído para a criação e proliferação mais eficaz da desinformação. Paralelamente, as democracias encontram-se particularmente vulneráveis a esta ameaça, a sua abertura facilita a proliferação de desinformação e a sua resposta é desafiada pela necessidade de salvaguardar a realização de princípios democráticos e direitos e liberdades fundamentais. Consequentemente, as democracias enfrentam um dilema de responder eficazmente à desinformação, por causa do seu impacto na vida democrática, sem comprometer direitos e liberdades fundamentais e prevenir assim a criação de outro tipo de inseguranças.

Neste contexto, este estudo usa a análise de discurso para analisar a *security governance* da desinformação online ao nível da UE. A UE entende a desinformação online como uma ameaça complexa e em constante evolução à sobrevivência do projeto europeu a todos os níveis, ao nível da segurança, político, económico e social. Adicionalmente, a UE reconhece o dilema de responder à desinformação, particularmente pelo facto de que esta pode ter várias formas e exige assim uma resposta calibrada. Deste modo, a União Europeia responde à desinformação online através da *democratic deterrence*, através de medidas de *denial* e de *punishment* para prevenir o sucesso da interferência e desafiar o cálculo estratégico do agressor.

Este estudo argumenta que a resposta da União Europeia é na sua maior parte proporcional, focada na proteção da liberdade de expressão em detrimento da proibição da desinformação. No entanto, as limitações subjacentes ao *Code of Practice*, à estratégica de *debunking* e à comunicação estratégica, bem como a inconsistência associada à recente suspensão de *media* Russos têm o potencial de ser explorados por adversários, com implicações para a eficácia da resposta. Assim sendo, apesar da União Europeia reconhecer o dilema de responder de forma eficaz e proporcional à desinformação online, o equilíbrio entre ambos é limitado, com implicações para o sucesso da resposta e para a própria proteção de direitos e liberdades fundamentais, que constitui o principal objetivo da resposta à desinformação online.

Palavras-chave: Desinformação Online; União Europeia; *Security Governance*; *Democratic Deterrence*; Eficácia; Proporcionalidade.

Abstract

This study analyses the consideration of the principle of proportionality in the response of the European Union (EU) to online disinformation as a security threat. The use of disinformation in politics it is not new, but the current political, economic, social and mostly the technological landscape allows for disinformation to be created and spread more effectively. At the same time, democracies are particularly vulnerable to this threat, their openness enables an easier proliferation of disinformation, and their response is challenged by the need to safeguard the realisation of democratic principles and fundamental rights and freedoms. Consequently, democracies face the dilemma of effectively responding to disinformation, because of its impact in democratic life, without jeopardizing fundamental rights and freedoms that can potentially generate other insecurities.

In this context, we use discourse analysis to analyse the security governance of online disinformation at EU level. The EU understands online disinformation as a complex and evolving threat to the survival of the European project at all levels, at the security, political, economic and social level. Furthermore, the EU recognises the dilemma of responding to disinformation, particularly because it may take multiple forms and thus demands a calibrated response. Therefore, the European Union responds to online disinformation through democratic deterrence, by measures of denial and punishment to prevent the success of interference and challenge the strategic calculus of the aggressor.

We argue that the response of the European Union is mostly proportional, focused on protecting freedom of expression rather than prohibiting disinformation. Nevertheless, the limitations underlying the Code of Practice, the debunking strategy and the strategic communications, and the inconsistency associated with the recent suspension of Russian media have the potential to be exploited by adversaries, with implications for the effectiveness of the response. Therefore, although the European Union recognises the conundrum of responding effectively and proportionality to online disinformation, this balance remains at crossroads, with implications for the success of the response and the protection of fundamental rights and freedoms itself, which is the main objective in responding to online disinformation.

Keywords: Online Disinformation; European Union; Security Governance; Democratic Deterrence; Effectiveness; Proportionality.

Table of contents

Acronyms

AI	Artificial Intelligence
APIs	Application programming interfaces
CSDP	Common Security and Defence Policy
EaP	Eastern Partnership
ECU	Eurasian Customs Union
EDMO	European Digital Media Observatory
EEAS	European External Action Service
ENP	European Neighbourhood Policy
ERGA	European Regulators Group for Audiovisual Media Services
EU	European Union
GDPR	General Data Protection Regulation
HR/VP	High Representative/Vice-President
NATO	North Atlantic Treaty Organisation
NGOs	Non-governmental organisations
OSCE	Organization for Security and Co-operation in Europe
UN	United Nations
US	United States of America

Introduction

This study analyses how the European Union has been taking into consideration the principle of proportionality in its security governance of online disinformation. There is a widespread concern with the competing interests of fighting harmful and deceiving content and the protection, respect and promotion of fundamental rights and freedoms, namely freedom of expression, considering its potential – of the response – to generate anti-democratic actions such as, for instance, censorship measures or even the privatisation of censorship. Hence, this study aims to understand how proportionality is considered in the equation to tackle online disinformation at EU level, in order to avoid exceeding the necessary to protect European democracy from this type of challenges and create other type of insecurities.

The use of disinformation in domestic and international politics it is not new. Nevertheless, the current political, economic, social and particularly the technological landscape have been creating fertile ground for an easier and a more efficient usage of disinformation, generating a greater attention both at the political as well as at the academic level. Today, with fewer resources and costs, disinformation campaigns can be disseminated more successfully. Thereby, disinformation campaigns, particularly disseminated online, have been considered a threat, specially to democracies, and have been placed at the top of the political agendas of democratic states and international organisations.

At the same time, the urgency to respond to this challenge by democratic states and international organisations has been accompanied by a dilemma underlying the effectiveness of the response of democracies to online disinformation without jeopardizing democratic values and principles and fundamental rights and freedoms. Yet, limited analytical attention has been paid to understand how democratic states and international organisations have been trying to cope with this conundrum of responding with proportionality.

The analysis concerning the balance between the response to online disinformation as a threat and the realisation of democratic values and principles and fundamental freedoms is important for two main reasons. The construction of something as a security problem is based on a sense of urgency and on the need to develop and implement exceptional measures (Buzan and Hansen 2009). Hence, constructing something in security terms may contribute to the design and implementation of policies that grant certain privileges to governments and legitimise the suspension of certain democratic principles and values and fundamental freedoms. Consequently, the relation between the realisation of security and the protection and promotion of human rights is complex and can be incompatible. Moreover, according to Bjola (2018), the absence of providing moral ground to act and the lack of proportionality in the response have the potential to contribute as part of the problem and as an amplifier of disinformation rather than a container. Consequently, the development and implementation of uninformed policies and strategies to address online disinformation that potentially challenge democratic principles and values may contribute to the success of disinformation campaigns by exposing the shortfalls of democracy and act as a multiplier of these campaigns.

Hence, there is an urgent need to focus the analysis on the response of democratic states and international organisations to online disinformation, considering the potential trade-offs between security and fundamental rights to be fertile ground for this threat to succeed. At the same time, a proportional response should not be designed at the expense of effectiveness, with the potential to deepen vulnerabilities of democracies in relation to these threats that may be further exploited by adversaries, as the COVID-19 pandemic crisis demonstrated with implications for the security, political and social landscape in Europe.

Thereby, this research contributes to understand the challenges underlying online disinformation from the point of view of the challenges underlying the response by democratic actors. Accordingly, the objective of this study is to analyse the response of the European Union (EU) to online disinformation in order to understand how the principle of proportionality is taken into consideration and we aim to answer the following question: *How does the European Union in its security governance of online disinformation takes into consideration the principle of proportionality?*

To this end, we apply discursive analyse methodology to the European Union, because we understand that this type of threat demands a response that states unilaterally cannot deliver, and the EU has become a central and an indispensable European security actor when it comes to the response to non-military threats such as disinformation (Jakobsen 2019).

To understand how the European Union discursively constructs online disinformation in security terms and normatively justifies its response to this type of challenge we use the concept of securitisation. In the analysis of the prerequisites and the structures involved in the response to online disinformation at EU level we use the conceptual framework of security governance. Moreover, we use the framework of analysis of moral authority proposed by Bjola (2018) and the four-type model proposed by Hellman and Wagnsson (2017) to identify the proportionality underlying the response to online disinformation at EU level and also the limitations and inconsistencies that have potential implications for the effectiveness of the response. But, is important to note that we do not aim to evaluate the implementation of the response.

In order to achieve the objectives and answer the research questions, this study is organised in six chapters.

The **first chapter** demonstrates the relevance and the innovation of analysing online disinformation as a threat from the point of view of the response, as well as introduces and justifies the conceptual and the methodological frameworks used to achieve the research objectives of this study. Hence, this chapter has three fundamental objectives.

Firstly, considering that the phenomenon of disinformation is not new, neither in domestic nor in international politics, we present the main discussions underlying disinformation as a threat and in particular online disinformation, to understand the changing dynamics underlying this phenomenon.

Secondly, this chapter introduces the research goals and the contribution of this study, namely by demonstrating the relevance and the innovation of analysing the challenge of online disinformation from the perspective of the response, particularly in democracies, considering the dilemma underlying the balance between the need to be effective without jeopardizing the realisation and protection of democratic values and principles and fundamental rights and freedoms.

Thirdly, this chapter presents and justifies the analytical framework namely the conceptual and the methodological frameworks. This study aims to be innovative also in terms of its operationalisation, by combining conceptual frameworks, we use three conceptual frameworks – security governance, securitisation and moral authority – and the analytical model proposed by Hellman and Wagnsson (2017). Moreover, we use a qualitative approach and we choose a social constructivist discourse analysis as method of interpretation and analysis.

The **second chapter** analyses the discussions in the literature underlying the understanding and construction of online disinformation as a threat, in particular to democracies, and has two fundamental objectives.

Firstly, this chapter analyses the discussions about the conceptualisation of disinformation and the elements that contribute to its dissemination and amplification.

Therefore, in order to understand the conceptualisation of disinformation in the digital era in security terms we analyse the conceptualisation of disinformation within the debate concerning the concept of fake news. Moreover, this study acknowledges the complexity of disinformation and its multiple origins, forms and implications. Accordingly, we analyse the dissemination and amplification of disinformation as resulting from an assemblage of technological, economic, political and psychological factors.

Secondly, this chapter also analyses the discussions about the construction of online disinformation as a threat, particularly to democracies. The use of disinformation in politics is not new, but today there is a widespread sense of urgency, particularly in democracies, to tackle this issue as a threat, thus, we aim to understand why is this the case.

In this context, this study aims to understand the underlying vulnerability of democracies to the threat of online disinformation. On the one hand, the openness of democratic societies is fertile ground for actors with malicious and harmful intentions to interfere through covert, subtle and non-military means in the form of disinformation, aiming at undermining internal cohesion and affecting the decision-making process. On the other hand, there is a sense of urgency in democracies to find strategies, tools and instruments to respond to these challenges without jeopardizing the same values that are under threat (Wigell 2021, pp.49-50).

Therefore, we aim to understand the motivations and the means employed to create and spread disinformation from perspective of the aggressor. Furthermore, we also aim to analyse the asymmetric disadvantage associated particularly with the open nature of democracies, in order to understand the conceptualisation and construction of online disinformation as a threat to democracies, namely within the framework of hybrid threats, cyber threats and as a threat to the democratic system.

The **third chapter** analyses the discursive construction of online disinformation in security terms at the EU level, in order to understand the normative justification of the European Union to act against online disinformation as a threat.

The preoccupation with the phenomenon of disinformation at the EU level is not new and has been mostly associated with the distance between the Union and its citizens. The political and the institutional complexity underlying the European Union has contributed to the relative distance between the Union and its citizens, which has been exploited by politicians to misinform and deceive on issues concerning the EU (Hedling 2021). However, despite the concern with the implications underlying the distance between the European Union and its citizens, only in 2015 has disinformation been officially recognised as a challenge to the foreign policy objectives of the Union. And, only since 2016 has it gained a prominent position in the political agenda of the Union and in security-focused initiatives (Carrapiço and Farrand 2020, p.1118).

In 2015, disinformation was recognised by the European Union as an external threat with origins in Russia to the strategic objectives of the Union in the eastern neighbourhood. Since 2016, the changing security landscape, the constant use of hybrid threats and cyber-threats in the form of disinformation and the various election processes occurring in Europe and in particular the 2019 European Parliament elections represented a turning point for the EU in terms of the rational underlying the discursive construction of disinformation as a threat. The dissemination of disinformation campaigns as a vehicle for hybrid threats was considered a mean to exploit the vulnerabilities and to manipulate the decision-making process of the European Union. Hence, beyond the rational of framing disinformation as a challenge to the realisation of the foreign policy objectives of the Union, disinformation came to be recognised as a "major challenge for Europe", as threat to European security and to the survival of the European project itself at all levels, political, economic and social.

Ever since, disinformation has been discursively constructed as a threat to European democracy, to the realisation of human rights and fundamental freedoms, but also as a threat to the realisation of the Digital Single Market and the European Digital Sovereignty and more recently with the COVID-19 pandemic crisis as a threat to public health.

Accordingly, the discursive construction of online disinformation as a threat at the EU level is not straightforward and this study identifies four main rationales that have been guiding this discursive construction: a strategic and security rational, a political rational, an economic rational, and more recently a public health rational. Despite these different rationales it is important to note that it does not mean that they occur separately, they influence and have implications for each other.

Therefore, in this chapter we aim to understand how and why has the European Union been understanding and constructing online disinformation as a threat and justifying its moral ground to respond to this challenge.

At the same time, the European Union has been recognising that disinformation may have multiple origins, forms and implications, demanding different security logics of response. Consequently, the EU understands that the threat of online disinformation requires a continuous assessment, a continuous adaptation and calibration of its response.

Accordingly, the European Union highlights that a calibrated response to interference and influence activities in the form of online disinformation should involve measures that deny the success of manipulation through the improvement of societal resilience. But, it should also involve measures that impose costs and punish the aggressor, in order to challenge its strategic calculus.

Therefore, the objective of **chapter four** is to understand how the European Union responds to disinformation, in particular we aim to identify the prerequisites underlying the security governance of online disinformation. Moreover, we also aim to understand what are the main elements that contribute to the option of democratic deterrence as a strategy to tackle online disinformation at EU level.

In **chapter five**, we aim to descriptively analyse the mains structures underlying the actions of denial that aim to tackle online disinformation as a threat to the foreign policy objectives of the EU in the eastern neighbourhood and as a hybrid threat to the European democratic, economic and social project, in order to evaluate the proportionality underlying the reaction of the EU to online disinformation.

In **chapter six,** we aim to descriptively analyse the main structures underlying the actions of punishment that aim to tackle online disinformation as a threat to the foreign policy objectives of the EU in the eastern neighbourhood and as a hybrid threat to the European democratic, economic and social project. Furthermore, we also analyse the overall response of the European Union to online disinformation in order to identify limitations and inconsistencies, with implications for the effectiveness of the response. Thus, the chapter also contributes to evaluate the balance between effectiveness and proportionality in the security governance of online disinformation at EU level.

CHAPTER 1

State of the Art, Research Goals and Analytical Framework

The use of disinformation in domestic and international politics is not a novelty. Nevertheless, the current political, economic, social and particularly the technological landscape have allowed an easier and a more efficient usage of this type of content, generating a greater attention both at the political as well as at the academic level. Today, with fewer resources and costs, disinformation campaigns are more successfully disseminated (Paterson and Hanley 2020, p.440; Wigell 2019). Consequently, the academic literature identifies at least three tendencies in terms of the potential effects of disinformation. First, disinformation contributes to increase polarisation. Second, disinformation contributes to increase distrust in traditional media and in democratic institutions. Third, disinformation impacts democracy more broadly and in particular political attitudes and the electoral process (Durach, Bârgăoanu and Nastasiu 2020, pp.5-6; Vériter, Bjola and Koops 2020, pp.571-572). Although the debatable effects of disinformation, disinformation campaigns disseminated online in particular, have been considered a threat, in particular to democracies, and have been placed at the top of the political agendas of states and international organisations.

The discussion underlying the response to disinformation has highlighted a widespread preoccupation that the fight against online disinformation may contradict democratic values and principles and fundamental rights and freedoms, namely freedom of expression. Consequently, generating an ethical dilemma with implications for the moral authority of democracies and for its capacity to effectively combat these campaigns (Althuis and Strand 2018, p.70; Bjola 2018, pp.306, 313; Omand 2018, p.12). Nevertheless, limited analytical attention has been paid to the approach to online disinformation (Saurwein and Spencer-Smith 2020), namely to evaluate the consideration of the principle of proportionality in the equation of the response.

Hence, this study aims to fill this gap, by analysing how the European Union has been taking into consideration the principle of proportionality in the security governance of online disinformation. The analysis focuses on the formulation of the response. In the first part, the study assesses the discursive construction of online disinformation in security terms and the normative justification to act against it at EU level. In the second part, the study analyses the level of reaction, namely by identifying the prerequisites - the interests, the objectives and the norms – and by describing the structures - the initiatives and the actors involved in the response to online disinformation, in order to assess the proportionality and accountability underlying the response to online disinformation at EU level. This study does not aim to evaluate the effectiveness of the implementation of the response of the Union, mostly because effectiveness is difficult to analyse and assess (Niemann and Bretherton 2013). Yet, considering that this study aims to also contribute to the discussions underlying the balance of effectively responding to disinformation without jeopardizing fundamental rights and freedoms we do identify some limitations and inconsistencies underlying the response of the of the European Union to online disinformation that may be exploit by adversaries and thus with implications for the effectiveness of the response.

This chapter has three main objectives. Firstly, it introduces the central discussions underlying disinformation and in particular online disinformation, and identifies the gap that this study aims to fill. Secondly, it presents the research goals and the contribution of this study, namely by demonstrating the relevance and the innovation of analysing the challenge of online disinformation from the perspective of the response. Thirdly, it presents and justifies the analytical framework, combining the conceptual and the methodological frameworks.

1.1. State of the Art

Online disinformation has gained increasing political and academic attention following events such as the Ukraine conflict in 2014, the 2016 Brexit referendum, the 2016 United States (US) Presidential elections, which has been reinforced following the COVID-19 pandemic crisis. This phenomenon has been studied by multiple disciplines such as communication and journalism studies, psychology, education studies, political science, international relations and security studies, and from different perspectives. This sub-chapter presents the central discussions underlying disinformation and particularly online disinformation, which have mostly been focused on the sources and patterns of distribution, and identifies the gap that this study aims to fill related with the analysis of the response.

This study understands disinformation within the umbrella of fake news, which despite its antiquity has not yet met consensus in terms of its definition. On the one hand, scholars such as McManus and Michaud (2018) and Tandoc Jr., Lim and Ling (2018) understand and analyse fake news as a concept that can acquire many forms. Depending on the degree of facticity and intention to deceive, it can be news satire, news parody, news fabrication, photo manipulation, advertising and public relations, propaganda up to misinformation and disinformation. Fake news has also been understood as genre blending by Mourão and Robertson (2019), as a concept that combines elements of traditional media with elements exogenous to professional journalism. On the other hand, other scholars' study fake news beyond a type of information and understand and analyse it as a floating signifier (Farkas and Schou 2018). In this context, fake news is analysed as a term that has been instrumentalised in political struggles (Jankowski 2018; Ross and Rivers 2018). The study of Egelhofer and Lecheler (2019) emerges as blending research of these two types of conceptualisation of fake news by suggesting the analytical framework of fake news as a two-dimensional phenomenon, as a genre and as a label[1]. Nevertheless, the genre label – type of false or misleading information used to deceive - has been getting more attention.

In this context, sources and patterns of distribution have been at the centre of the analysis. Accordingly, the usage of online disinformation in Russian foreign policy has gained more attention (Averin 2018; Mejias and Vokuev 2017). Nevertheless, scholars such as Ross and Rivers (2018) and McGonagle (2017) demonstrate that the use of disinformation is not only limited to Russia and neither to state actors. Moreover, despite the attention that online disinformation has been received particularly as a foreign policy tool limited attention has been paid from International Relations theories. La Cour (2020) tries to fill this gap by exploring the contribution of different concepts of International Relations theories to understand contemporary usages of digital disinformation, such as E.H. Carr's notion of propaganda, John J. Mearsheimer's typology of lies and Joseph Nye's concept of public diplomacy.

Further studies focus on the elements that contribute to the successful proliferation of disinformation with particular attention to the role of digital technologies, namely on the exploitation of the technical features of social media such as algorithms, filter bubbles, echo chambers (Dooley, Moore and Averin 2018; Prier 2017). Furthermore, Bakir and McStay (2017) highlight the role of the economic dimension underlying the use of algorithms that contributes to the economy of emotions. Accordingly, it is argued that the success of the dissemination of disinformation lies on the exploitation of emotionally targeted news highlighted by algorithms, which is associated with the economic model of social media.

Notwithstanding, according to Saurwein and Spencer-Smith (2020), not only technological, but also political, social and psychological elements are important to consider in order to understand the success in the proliferation of disinformation (p.823). Hence, Bennett and

[1] This will be further discussed in chapter two.

Livingston (2018) analyse the underlying factors that have contributed to the current disinformation order. The growing legitimacy problems in democracies, the increasing distrust and citizen declining confidence in democratic institutions are important elements that contribute to the pursue for alternative sources of information, particularly online (Bennett and Livingston 2018). Moreover, Waisbord (2018) reinforces this argument by identifying fake news as a symptom of the collapse of the traditional news order and contemporary public communication chaos marked by a struggle over the definition of truth. Furthermore, other studies highlight the role of the audience, by analysing the psychological and mental process that explain the consumption, acceptance and integration of disinformation campaigns, namely the mental process of confirmation bias (Ling 2020; Mayo 2019; Ray and George 2019; Nelson and Taneja 2018).

Yet, the patterns of distribution and the effects of disinformation campaigns are not linear. Humprecht (2018) compared the dissemination of these campaigns across four Western democracies and concluded that the format and the content tend to adapt and is shaped by the national information and political environment.

Other studies discuss the effects and implications of online disinformation, which can have an impact in peaceful as well as in conflict situations. On the one hand, Steensen (2019) highlight the negative impact of disinformation in journalism, but at the same time sees it as an opportunity to lead journalism towards an epistemic reorientation particularly in terms of deepened the criticism of the source. On the other hand, Clements (2014) analysed the use of disinformation in scenarios of military conflict and studied the possible implications that these campaigns may have in distortion the adversary's perception of its ability and contributing to surrender.

Nevertheless, the effects of disinformation on politics have been mostly contested. Whereas Paterson and Hanley (2020) argue that the digital age reinforced the use, changed permanently the way states conduct these operations and has a high destabilising effect (p.439). Allcott and Gentzkow (2017) analyse the relation between social media and politics, with focus on the 2016 US Presidential elections, and conclude that the impact of these campaigns on voting patterns is limited. Moreover, according to Guess, Nagler and Tucker (2019), the prevalence and dissemination of fake news in the 2016 US Presidential elections is a rare activity.

At the international level, Lanoszka (2019) and Gerrits (2018) studied disinformation in international politics and criticize the hype underlying disinformation as a security threat. Accordingly, disinformation shouldn't be overstated as a security threat considering that is ineffective in terms of influencing change in the political alignments of the target in terms of foreign policy and defence matters, thus with little implications in the balance of power.

Notwithstanding, despite the debatable effects that online disinformation may have in domestic and international politics, states and international organisations have been framed disinformation as a threat namely to democracy. Yet, there is little attention and limited clarity on what it actually means for disinformation to threaten democracy. Tenove (2020) tries to fill this gap by demonstrating the challenge that disinformation poses to three normative goods of the democratic systems, namely self-determination, accountable representation and public deliberation and the policy responses that should be developed and implemented accordingly.

As far as it concerns to the analysis of the response to online disinformation the majority of studies have focus on the identification and description of measures that should be taken in order to address this challenge. Bjola and Pamment (2016) suggest the implementation of a strategy based on digital containment, which lies on the support to media literacy, institutional resilience and strategic narratives. Roozenbeek and van der Linden (2018) reinforce the idea of the need to focus on education by suggesting educational games as a mean to inoculate citizens against fake news.

Wigell (2021) believes that democracy is both a vulnerability to interference, but also the key to the fight against it. Accordingly, he suggested a broader strategy towards this type of interference by proposing democratic deterrence. Accordingly, democracies should deter the adversary from interference through denial and punishment. On the one hand, the strategy of denial is based on the idea of mitigating the vulnerabilities that allow the success of the proliferation of these types of campaigns through the improvement of the resilience of democracy. On the other hand, the strategy of punishment aims to punish for having interfered, namely through sanctions, by exposing these campaigns and by promoting democracy (Wigell 2021, pp.55-63).

Further studies analyse regulation as a tool to fight online disinformation, particularly the regulation of social media platforms (Althuis and Strand 2018). At the international level, analysis have also highlighted the need for an international legal framework to regulate state use of these type of tactics on social media (Baade 2019; Nicolas 2018). Nevertheless, similar to other new threats, there is a widespread concern that measures such as regulation may have direct implications to the protection and promotion of fundamental values and principles such as freedom of expression, raising complex dilemmas for liberal democracies to balance security and civil liberties (Wigell 2021; Chappell, Galbreath and Mawdsley 2019; Althuis and Strand

2018; Bjola 2018). Bjola (2018) suggest the concept of moral authority as a possible toolkit to surpass this ethical dilemma.

However, despite this preoccupation limited studies have been focused on analysing whether and to what extent can the responses of democratic states and international organisations jeopardize the protection and promotion of fundamental democratic values and principles. The focus has been on descriptively analysing the measures taken by states and international organisations (Saurwein and Spencer-Smith 2020; Schia and Gjesvik 2020; Polyakova and Fried 2019).

In the case of the European Union, efforts have been made in order to go beyond a descriptively analysis of the policies and strategies to address online disinformation.

On the one hand, some studies focused on the analysis of the response and conclude that it is not linear and has two distinct value-perspectives. Whereas the security-defence and internet perspective value coherence and efficiency, the education and media perspective value the independent democratic judgment of the citizens (Ördén 2019).

On the other hand, some scholars explore the implications of the fight against online disinformation in the decision-making process of the EU. Accordingly, for instance, the approach of the EU towards online disinformation is accompanied by a rupture in the relationship between Brussels and the private sector, namely with social media platforms, which are not seen as trustworthy and demand greater oversight (Carrapiço and Farrand 2021; Carrapiço and Farrand 2020). Moreover, according to Hedling (2021) the fight against disinformation also had implications regarding the transformation of the practices of diplomacy.

As far as it concerns the relationship between the response of the EU to the threat of online disinformation and the protection and promotion of democratic values and fundamental rights and freedoms the analysis has been limited. Wagnsson and Hellman (2018) contribute to closing this gap by analysing the implementation of the tasks of the East StratCom Task Force, namely through Disinformation Digest. They conclude that it may challenge the Normative Power of the EU, considering the antagonistic representation of Russia in the Disinformation Digest. Accordingly, in Disinformation Digest Russia has been represented as the 'other' and antagonically, "as inferior, as a threat, and as a violator of universal norms" (Wagnsson and Hellman 2018, p.1170). Hence, these counter-narratives in direct response to an external adversarial narrative follows an offensive confronting approach and it also contradicts the European model of normative power. A normative power "should communicate in a non-antagonistic, humble way and avoid constructing others in ways that sustain hierarchies that can stir conflict" (Wagnsson and Hellman 2018, p.1161). Consequently, by employing a confronting approach, trough Disinformation Digest, the EU uses an 'othering' strategy, that creates an antagonistic division between 'us' and the 'other', which can contradict its normative power and prompt conflict situations. Nevertheless, not only does the study reflects only a limited part of the action of the EU to online disinformation, but is also limited in the contribution in terms of the impact on the protection and promotion of democratic values and principles remains limited.

Hence, the starting point of this study is that besides the concern with the potential implications of the response to the threat of online disinformation for the protection and promotion of democratic values and fundamental rights and freedoms, limited attention has been paid to analyse the response of liberal democracies, in this case of the European Union.

1.2. Research Goals: the need to analyse proportionality in the security governance of Online Disinformation at EU level

This sub-chapter clarifies the contribution, the relevance and the innovation of studying proportionality in the security governance of online disinformation by the European Union.

This study offers an alternative, relevant and innovative way to study online disinformation reflected in two central aspects, in terms of conceptualisation and operationalisation.

First, it provides an alternative conceptualisation of the challenges and threats associated to online disinformation through the analysis of the response. The conceptual and empirical analysis of online disinformation in security terms has been focused mostly on the source, the tactics and patterns of distribution of this type of information. As far as it concerns to the analysis of the response, studies have been centred on introducing measures that should be taken in order to mitigate this challenge and on the description of policies taken by states and international organisations.

In this context, despite multiple governments and international organisations have come to understand and address online disinformation as a threat, there persists a lack of clarity in political debates and academic literature concerning what it actually means for online disinformation to threaten democracy. Clarifying the construction of online disinformation as a threat is important to identify, develop and implement informed and proportional policy responses and prevent the proliferation of other insecurities (Tenove 2020).

The complexity underlying the conceptualisation of online disinformation as a threat has been accompanied by a widespread concern with the balance between the fight to harmful and deceiving content and the protection, respect and promotion of fundamental rights and freedoms, namely the freedom of expression. Multiple studies have been highlighting the potential for censorship in the response to online disinformation, namely the privatisation of censorship, this is the delegation to online platforms of the process of balancing fundamental rights online (Helm and Nasu 2021; Monti 2021; Sardo 2020). But also, political actors such as international organisations as the European Union and the United Nations (UN) have demonstrated preoccupation with the need to protect, respect and promote human rights and fundamental freedoms in the response to this threat. This is manifested in the multiple official documents that will be analysed at EU level in this study, but also in the Report of the United Nations Secretary-General on "Countering disinformation for the promotion and protection of human rights and fundamental freedoms" (2022) which specifically mentions the need to protect, respect and promote freedom of expression, avoid imposing disproportionate sanctions and never criminalise legitimate content, and refrain from internet shutdowns and/or blocking of websites. Addressing online disinformation has the potential to contradict fundamental democratic values and principles, and consequently generate difficult trade-offs between security and fundamental rights. Yet, limited attention has been paid beyond the descriptively identification of measures taken by democracies to address the challenge of online disinformation.

In this context, studying the principle of proportionality in the response to online disinformation emerges as useful to understand how political actors can deal with this dilemma. Proportionality as a principle of law is rooted in the Aristotelian concept of justice and has been predominantly used in the context of human rights protection and humanitarian law, the use of force and countermeasures, maritime boundary law, trade law and investment protection (Cottier et al. 2017, p.628; Engle 2012, p.10[2]). According to Cottier et al. (2012) "proportionality is being used to assess whether restrictions and measures affecting human rights appropriately respond to legitimate public interests" (p.5).

Studying the principle of proportionality in the response to online disinformation is appropriate to evaluate the balance of competitive interests of fighting disinformation and protecting, respecting and promoting human rights, but also important for two main reasons.

[2] In order to have a detailed understanding of the historical evolution of the principle of proportionality see, for instance, Ucaryilmaz (2021) and Engle (2012).

First, according to Buzan and Hansen (2009), the construction of something as a security problem is based on a sense of urgency and the need to develop and implement extreme measures. This construction may result in problematic or dangerous policies that grant certain privileges to governments and legitimise the suspension of certain democratic principles and values. In this regard, the challenging relation between security and human rights is not new. Moreover, according to Bossong and Hegemann (2019), internal security should not be understood and used as a neutral term, because there are competing interpretations related with the boundary between security and freedom, which may contribute to securitisation politics (p.101). Second, and following the previous reason, according to Bjola (2018), "failure to maintain moral authority could make an actor vulnerable to accusations of serving to amplify rather than contain disinformation, and thus help to legitimize the claims of those intentionally promoting disinformation" (p.306).

The relevance and the innovation of this study lies in the assumption that the response to online disinformation may function as a fertile ground for this threat to succeed. The development and implementation of uninformed policies and strategies to address online disinformation that potentially challenge democratic principles and values may contribute to the success of disinformation campaigns by exposing the shortfalls of democracy and act as a multiplier of these campaigns. Therefore, this study aims to fill this gap, by analysing the normative justification of the European Union to respond to disinformation and the proportionality of the security governance of online disinformation at EU level.

Thereby, the research goal of this study is to analyse the consideration of the principle of proportionality underlying the security governance of online disinformation at EU level and it answers the following question: *How does the European Union in its security governance of online disinformation takes into consideration the principle of proportionality?*

In order to achieve the research goal of this study and answer the defined research question, and informed by the proposal of Christou et al. (2010) to understand the interaction between the logics of security and governance at EU level, this study identified the following sub-research goals and questions:

- The sub-research objective one is to understand the discussions on how and why online disinformation has become to be understood and analysed in security terms, and answers the following question: *How and why online disinformation has been constructed and analysed as a threat? (Chapter 2)*
- The sub-research objective two is to understand how and why online disinformation has been discursively constructed in security terms by the European Union, and answers the

following questions: *How does the European Union discursively constructs online disinformation in security terms? How the European Union normatively justifies the need to respond to online disinformation? (Chapter 3)*

- The sub-research objective three is to understand what strategy has the European Union defined to respond to online disinformation and its underlying reasons, and answers the following questions: *What sort of security logic was constructed by the European Union for the security issue of online disinformation, considering its understanding of the main elements that contribute to its proliferation and resilience? What prerequisites, goals and norms have the European Union discursively defined to address online disinformation as a threat to the foreign policy objectives in the eastern neighbourhood in terms of measures of denial and punishment? What prerequisites, goals and norms have the European Union discursively defined to address online disinformation as a hybrid threat to the European democratic, economic and social project in terms of measures of denial and punishment? (Chapter 4)*
- The sub-research objective four is to understand the consideration of the principle of proportionality in the security governance of online disinformation at EU level through measures of denial and its implications on the overall security governance of online disinformation, and answers the following question: *What structures of security governance have resulted from constructing online disinformation as a threat? What denial initiatives have been defined by the European Union to respond to disinformation as a threat to the foreign policy objectives in the eastern neighbourhood? Which actors are involved in these structures? What denial initiatives have been defined by the European Union to respond to disinformation as a hybrid threat to the European democratic, economic and social project? Which actors are involved in these structures? (Chapter 5)*
- The sub-research objective five is to understand the consideration of the principle of proportionality in the security governance of online disinformation at EU level through measures of punishment and its implications on the overall security governance of online disinformation, and answers the following question: *What punishment initiatives have been defined by the European Union to respond to disinformation as a threat to the foreign policy objectives in the eastern neighbourhood and as a hybrid threat to the European democratic, economic and social project? Which actors are involved in these structures? Which type of action – confronting, blocking, naturalising or ignoring – better describes the strategy underlying the security governance of online disinformation at EU level? How does the*

security governance of online disinformation at EU level considers proportionality? (Chapter 6)

Second, in terms of operationalisation, the innovation of this study also lies in the combination of three conceptual frameworks – security governance, securitisation and moral authority – and the analytical model proposed by Hellman and Wagnsson (2017).

The increasing widespread digitalisation and interconnectedness of contemporary societies demands "governance in networks, which in turn means that governments increasingly share responsibility with actors from business and society" (Cavelty and Wenger 2020, p.24). Consequently, online disinformation, similar to other new security threats, is complex and involves multiple dimensions and areas of action, therefore demanding the integration of multiple actors beyond national governments. In this scenario, security governance offers an alternative perspective to analyse this type of fragmented forms of governance of security.

Security governance is an analytical concept and a political practice. As an analytical concept, security governance studies fragmented forms of policy-making and implementation that emerged in the post-Cold war era in the field of security. As a political practice and a prescriptive concept, security governance is considered a 'heuristic device' and makes normative claims, based on the assumption that certain prerequisites (shared interests and goals, and norms and ideas) and structures (multiple actors, de-centralised modes of cooperation, and voluntary compliance mechanisms) generates effectiveness and legitimacy (Ehrhart, Hegemann and Kahl 2014a, p.148). This study uses security governance as an analytical concept, with particular attention to prerequisites and structures.

Nevertheless, security governance is limited in terms of analysing how the understanding of security and security issues emerge, thus this study proposes to use the literature on securitisation in order to fill this gap.

In addition, considering the objectives of this research concerning the evaluation of the relation between the formulation of the response to online disinformation and the realisation of democratic principles and values, this study uses the concept of moral authority proposed by Bjola (2018) and the analytical model proposed by Hellman and Wagnsson (2017).

1.3. Conceptual Framework: Security Governance, Securitisation, Four-Analytical Model and Moral Authority

This sub-chapter presents and justifies the conceptual framework that guides the analysis of the response to online disinformation at the EU level and its relation with the realisation of democratic principles and values.

This study combines three conceptual frameworks – security governance, securitisation and moral authority – and an analytical model proposed by Hellman and Wagnsson (2017).

The adoption of the conceptual framework of security governance to analyse the response to the threat of online disinformation and its application to the European Union case study is justified by two central arguments.

First, online disinformation is a complex challenge with multiple facets and implications, consequently, demanding a response that goes beyond the state level and traditional security and defence structures, initiatives and instruments. Therefore, security governance emerges as a suitable conceptual framework, because it captures the changes in the threat landscape feature of the post-Cold War era, particularly the emergence of new security threats, and the subsequent dynamic changes in the management of security, characterised by the presence of multiple actors and multiple levels of security coordination, management and regulation (Kirchner 2006, pp.948, 965). In this scenario, the emergence of new security threats, which are more complex and multi-faceted, is accompanied by a response that goes beyond the state and the military level. Whereas during the Cold War period European security was mostly confined to the defence sector, today the emerging threat landscape demands the participation of multiple sectors and actors (Chappell, Galbreath and Mawdsley 2019, p.10).

Second, the employment of the security governance framework to the case study of the European Union[3] is particularly useful because, according to Christiansen (2013), governance has been used as a way to overcome the challenge underlying the categorisation of the EU in terms of the traditional distinction between international system and nation-state. The governance framework has been recognised as an alternative to refer to the decision-making process at EU level without signalling a potential path of becoming a state. The idea of statehood at European level has been contested and undesirable, particular in terms of popular acceptance, however in the early 2000s the taboo underlying the application of the notion of

[3] There have been three main different usages of the concept of the governance to study the European Union: multilevel governance approach, the new governance approach and the study of new modes of governance. The multilevel governance approach considers a multiplicity of actors on a variety of territorial levels, not only national but also local entities have an impact in the policy-making at EU level; the new governance approach understands the EU as a 'regulatory state'; and the study of new modes of governance relates to the use of non-binding instruments in the policy-making in the EU (Christiansen 2013, p.104). We believe that the understanding underlying the study of new modes of governance is more appropriate to this study.

nation-state to the EU was broken. However, the Lisbon Treaty changed statehood linguistics because it was highly problematic. Hence, the use of governance in European politics more broadly became appealing and has been widespread used as an alternative. Besides, the concept of governance not only offers an alternative to surpasses the problem of categorisation, but it also captures the particularities associated with the European construction, which will be further discussed in the sub-chapter four about the methodological framework (Christiansen 2013), pp.103-104, 106).

Furthermore, the conceptual choice of the security governance framework is also justified by its analytical contribution to the research objective in terms of supporting the identification, analysis and description of what the European Union does, particularly in terms of the response to the threat of online disinformation, rather than how the Union emerged. Additionally, this analytical framework understands the EU as an independent variable and focuses on the description of the process of achieving outputs rather than on the outputs (Christiansen 2013, p.104).

Nevertheless, despite the added value of security governance to the research objectives of this study, particular to describe the response of the EU to online disinformation and the involvement of multiple actors, there are scholars that criticize the concept, particularly the potential incompatibility between governance practices and traditional democracy[4], which may be perceived as an indirect form of jeopardizing democratic values and principles in the response to online disinformation. Whereas some scholars highlight the potential normative benefits of governance, namely greater deliberation and inclusiveness in the policy process as well as advantages of depoliticized regulatory activity (Christiansen 2013, p.112), others have been critical of security governance, arguing that it has been employed mainly in a descriptive manner, reproducing only a positive perspective of the cooperative process and problem-solving capacities, neglecting important aspects related to the coordination process (such as its inclusiveness, hierarchy-free and voluntary) (Ehrhart, Hegemann and Kahl 2014a, p.150). Accordingly, there has been criticism over a tendency to presume that security governance is efficient and that power relations between actors follow harmoniously within governance

[4] For a deeper understanding of the discussions underlying the pitfalls of the concept of the security governance see, for instance, Ehrhart, Hegemann and Kahl (2014b) and Sperling and Webber (2014). Ehrhart, Hegemann and Kahl (2014b) highlight the challenges associated with the flexibility of the concept, particularly the governance dimension; with the application of the concept to specific policy fields; and with the normative dimension. Moreover, Kavalski (2008) notes that security governance does not consider the complexity underlying the alterations in the meaning and practices of global life, suggesting the concept of complex security governance.

structures (Sperling and Webber 2014, p.129). Consequently, Ehrhart, Hegemann and Kahl (2014a) argue that security governance should be reframed as a critical tool, that does not take existing institutions, arrangements and power relations for granted but questioning how they emerged (p.150).

Moreover, considering the potential incompatibility between governance and traditional liberal democracy at EU level, Christiansen (2013) notes that critics of the governance approach argue that multiple governance practices at EU level in the form of regulatory decisions have significant societal implications and may favour certain Member States, groups or sectors. This type of decisions demand legitimation in terms of representative democracy, evidencing a potential difficulty in reconciling new forms of governance with traditional liberal democracy (p.110). Furthermore, the participation of the European civil society in European politics is usually operationalised through Non-governmental organisations (NGOs) based in Brussels, which are in most cases dependent on financial support from the European Commission, raising doubts over the representativeness of the European civil society. Consequently, Ehrhart, Hegemann and Kahl (2014b) argue that there are some alerts with potential implications for the realisation of democratic accountability and human rights, which challenges the inherent normative dimension of security governance, that assumes that the governance framework is the most appropriate approach to address challenges in the post-Cold War era and the path that provides effective and legitimate coordination (pp.122-123). Hence, critics of the governance framework have been arguing that the theoretical advantages underlying this approach do not materialise in practice (Christiansen 2013, p.112).

Despite the potential added value to assess the fulfilment of democracy principles and values in the internal policy-making process of the response to disinformation, as an additional path to evaluate the moral authority of the EU, the research objectives of this study do not aim to proceed with this path. The research interest in the emergence of prerequisites and structures is focused on the identification of the interests, objectives, norms and ideas (prerequisites) and initiatives and actors (structures), rather than on how they emerged following power relations between actors involved in the policy-making process underlying the response to online disinformation.

Additionally, another pitfall that has been identified in relation to the concept of security governance concerns the assumption that it has been based predominantly on the understanding of the dynamics of governance, involving multiple actors, tools and instruments, whereas the complexity of security, particularly the construction of the meaning of security has been neglected. Thus, in order to better understand the European Union in the field of security and as a security actor, it is important to analyse how the EU constructs its understanding of security and thus its security practice, particularly in relation to online disinformation. Hence, the security governance concept benefits from the incorporation of the conceptual framework of securitisation, which provides "a more complex understanding of the way in which security comes to be understood and intersubjectively defined, which in turn has implications for the relevant actors involved, governance/governmentality strategies and policy practice" (Christou et al. 2010, pp.344-345).

Securitisation refers to the discursively construction of security, hence is the intersubjective socio-political process of discursively framing an issue in security terms. In this context, securitising actors present an issue as posing an existential threat to a particular referent object (Vuori 2017, p.65; Balzacq 2010, p.59; Emmers 2010, p.137; Buzan and Hansen 2009, p.212). Therefore, the introduction of this conceptual framework benefits the analysis, because securitisation clarifies the discursive construction of online disinformation as a threat at the EU level as well as its normative justification to act against it.

As previously mentioned, this study is not interested in the analysis of the implementation and effectiveness of the response to online disinformation at EU level. Thus, we believe that instead of focusing on the element of effectiveness and legitimacy of the security governance framework the research benefits from the use of the analytical model proposed by Hellman and Wagnsson (2017) and the concept of moral authority proposed by Bjola (2018).

On the one hand, the analytical model proposed by Hellman and Wagnsson (2017) benefits the analysis because it allows the characterisation of the response to online disinformation adopted by the European Union. This model considers four possible strategic paths to address online disinformation: confronting, blocking, naturalising and/or ignoring. In this context, some strategic options are more in accordance with democratic principles and values than others. Hence, with implications for the moral authority of the EU concerning the response to online disinformation, particularly, it helps to inform the analysis underlying the strategic consideration, which refers to the level of reaction to a particular issue.

On the other hand, the analytical concept of moral authority proposed by Bjola (2018) allows the evaluation of the moral ground guiding the response to online disinformation at the EU level. The concept of moral authority emerges as a toolkit to address the dilemma of responding to online disinformation without contradicting fundamental democratic principles and values. Accordingly, the response to online disinformation should consider three elements that nourishes moral authority, it "needs to make the case that is has been harmed, that it has normative standing to engage in counter-interventions, and that it does so in a proportionate and responsible manner" (Bjola 2018, p.313). Thus, the evaluation of the realisation of these three elements allows the analysis of whether the response to online disinformation at the EU level has been informed by moral authority and thus surprising the ethical dilemma mentioned above.

1.3.1. Security Governance and the Contemporary Security Landscape: new threats, new actors and new forms of coordination

Security governance has its origins in the late 1980s and early 1990s, but in Europe it first emerged in the early 2000s as an alternative understanding of contemporary international security that arise following the end of the Cold War and the consequent collapse of the bipolar world. Security governance emerged as an analytical concept and a political practice to deal with the new security landscape and the new security practices that followed (Bevir, Daddow and Hall 2014; Kirchner and Sperling 2007; Krahmann 2005a). This sub-chapter aims to introduce the context – new security threats, new actors and new forms of coordination – that contributed to the emergence of the concept of security governance.

Traditional International Relations theories, such as Realism, assume that international relations are marked by actions and interactions of sovereign states that pursue their national interest through the maximization of economic and military power. In this scenario, the main security threat is interstate conflict and military threat, and international security is achieved through the balance of power and alliances. Moreover, the security of the state means the security of its citizens and communities. However, the security of the state does not necessarily translate into the security of its citizens, considering that often sates are the main aggressor, and the new transnational security threats demand new modes of security provision that goes beyond traditional state-centric responses[5] (Bevir, Daddow and Hall 2014, p.1).

The combination of the new security threat landscape and the changes in the European state system since the 1950s, accelerated by the end of the Cold War, demanded an alternative understanding of contemporary international relations, particularly concerning the dynamics underlying the provision of security (Kirchner and Sperling 2007, pp.18,20). Consequently, security governance arises as a conceptual and prescriptive reaction to the shift towards a complex international security threat landscape, marked by risks, actors and mechanisms that extend beyond traditional, state and military-centred security policy, exposing the inadequacies

[5] To deepen the understanding of the debates concerning the evolution of Security Studies see, for instance, Duque, Noivo and Almeida e Silva (2016); Collins (2010); Buzan and Hansen (2009).

of traditional practices and demanding more flexible multi-level and multi-actor methods (Hegemann and Kahl 2016; Ehrhart, Hegemann and Kahl 2014b; Ehrhart and Petretto 2014). The emergence of this concept is mostly associated with three principal assumptions concerning the changes noticed in contemporary international relations. First, states are no longer the primary source of threat and the contemporary international security threat framework has been marked by the complexity of new challenges and threats namely of transnational character. Second, the character of the new risks and threats pressures traditional state capabilities and exposes the inadequacy of sovereignty-bound policy-making, contributing to the emergence of new actors entitled of providing security. Third, and related with the previous is the emergence of new forms of coordination based on the assumption that the provision of security is guided by cost-efficiency, thus demanding the need for the state to cooperate with other actors in the provision of security (Kavalski 2008; Krahmann 2005a).

Firstly, the emergence of security governance is largely associated with the new security threat framework that emerged during the 1980s and the 1990s (Kirchner and Sperling 2007, p.18). The end of bipolarity – superpower confrontation – and the subsequent decreasing likelihood of interstate war, the re-emergence of dormant conflicts in developing countries, and the effects of globalisation, meaning that local challenges and problems can have global effects, contributed to a new security landscape. Consequently, the academic discussion on the utility and appropriateness of broadening and deepening the concept of security was accompanied by an amplification of threat perception by governments and international organisations in the European and transatlantic region (Ehrhart, Hegemann and Kahl 2014a, p.147; Krahmann 2005a, pp.16-17).

The 1980s and the 1990s were marked by the widening and deepening of the security agenda, translated namely by the works of Barry Buzan. On the one hand, Buzan (1997) suggested the widening of the security threat framework beyond the military sector to also accommodate the political, economic, environmental and societal sectors. On the other hand, the deepening of security referred to the consideration of the individual level. Moreover, the concept of securitisation introduced by Ole Waever (1995) complemented the discussion by identifying the broadening of the security threat landscape and the scope of actors involved in the provision of security.

Contemporary security threats against the state are mainly indirect, considering that they target mostly the society and the ability of the state to fulfil the social contract rather than its ability to govern (Kirchner 2007, pp.5-6; Kirchner and Sperling 2007, pp.6-7). This is associated with the evolution of the territorial state – Westphalian state – towards a post-

Westphalian state more open and vulnerable to new categories of threat. The contemporary international system encompasses Westphalian and post-Westphalian states. The traditional Westphalian state is mainly concern with territorial integrity and political sovereignty; whereas the post-Westphalian state, despite is preoccupation with territorial integrity, is mainly focused on maximizing economic and social welfare and it is dependent on external cooperation to achieve that objective. As a consequence, the increasing disappearing of traditional borders and the openness of post-Westphalian state means that not only are national governments vulnerable to traditional threats to territorial integrity, but they are also pressured by new transnational threats (Kirchner and Sperling 2007, pp.3-4). In this scenario, the state is no longer the only source of threat nor the only target, generating a need to broaden the concept of security beyond the military sector and also a deepened of the levels of analysis, beyond the state to also include individuals, communities, humanity and the planet itself (Christou et al. 2010, p.343; Krahmann 2005b, p.531). Therefore, particularly in the European context, the centrality of the military threat that characterised the Cold War era has been replaced by an attention towards other types of threats already prevalent in other parts of the world, such as the resurgence of ethno-nationalist political violence in the post-Soviet space and in global South, civil war, new forms of conflict fought by irregular forces not bound to international humanitarian law or basic riles of war, terrorism, transnational crime, and human trafficking. Moreover, there has been a growing awareness of transnational security threats and risks related to cyberspace, climate change and poor governance (Bevir and Hall 2014, p.18; Sperling and Webber 2014, pp.127-128). Additionally, at the same time interstate war is declining in frequency as the resulting number of causalities, meaning that security threats are neither mainly military nor addressed through pure military means (Sperling and Webber 2019, pp.233-234; Christou et al. 2010, p.343; Krahmann 2005b, p.537). Consequently, the widening of the security threat landscape and the inclusion of new risks and threats was accompanied by an alternative type of response characterized by the broaden of the scope of actors and the instruments that provide security (Ehrhart and Petretto 2014; Sperling and Webber 2014).

Therefore, secondly, the rise of the security governance concept is also related with the emergence of new security actors. Accordingly, it is assumed that the state is no longer neither the primary source of threat nor the only actor capable of providing security (Sperling and Webber 2019; Krahmann 2005a). The complexity underlying contemporary security challenges not only pressures the capacity of national governments to address them unilaterally, but it also exposes the limits and inadequacy of traditional sovereignty-bound policy-making arrangements to address the new security threat landscape. Consequently, an increasing number of new actors have emerged to address security issues such as humanitarian aid, human rights monitoring, refuges, and military training and protection (Ehrhart, Hegemann and Kahl 2014b; Christou et al. 2010; Kirchner 2007; Krahmann 2005a).

The transnational character of the majority of contemporary security threats contributed to the relying of states on intergovernmental organisations such as the United Nations (UN), the North Atlantic Treaty Organisation (NATO) and the EU to address these issues. This phenomenon is not a novelty; however, the outsourcing of security has deepened, with states transferring greater powers to international organisations to address collective action problems; and widened, with states not only outsourcing security to intergovernmental organisations, but also collaborating with Non-Governmental Organisations, private military companies, private sector and other non-state actors. The state maintains the legitimate monopoly of the use of force and coercive means, however in the complex contemporary security environment that capability is no longer the most important (Sperling and Webber 2019, pp.233-234). States maintain a key role in the production of security, however, they have to manage their efforts in coordination with the increasing number of international organisations and non-state actors, which are occupying a crucial position in the making and implementation of international policies, including security policies, a traditional domain of national governments (Ehrhart, Hegemann and Kahl 2014b, p.119; Kirchner 2007, pp.5-6; Krahmann 2005b, p.531). Nevertheless, according to Sperling and Webber (2019), this shift in the role of the state cannot be reduced to a transference of power and authority to other actors in order to address complexity. Considering that on the one hand, some states have address complexity by delegation of functions to subnational governmental bodies, private actors, and international institutions; and, on the other hand, other states resisted this transference, such as China, Turkey, Russia and the United States of America under the administration of President Donald Trump.

In the European and transatlantic region, the shift in threat perception was accompanied by a growing fragmentation of security policy-making, as a result of limited resources, lack of expertise in non-traditional security threats as well as divergent interests among governments. Hence, nowadays, despite the continuous key role of states and governments, we witness a growing engagement of international institutions and non-state actors such as non-governmental organisations and the private sector in the provision of national and international security. It is important to note that this assumption does not mean that states are being replaced by non-state actors, but that states, in order to approach emerging transnational security threats and to compensate the decreasing public budget for security, are making and implementing new forms of coordination. Consequently, the complexity of the security landscape and the rising costs associated with national and international security and defence means that these actors can be an added-value and offer additional resources and expertise (Ehrhart, Hegemann and Kahl 2014a, p.147; Krahmann 2005a, pp.17-18, 23).

Thirdly, these changes in the international system – new risks and challenges and new actors – were translated into the need for effective and efficient problem-solving solutions that should be pursued through a system of international governance (Hegemann and Kahl 2016; Bevir and Hall 2014; Kohler-Koch and Rittberger 2006). Accordingly, "state legitimacy is no longer based on the monopoly on the provision of national and international security, but increasingly the cost-efficient delivery of security" (Krahmann 2005b, p.537). Therefore, governance emerges as a framework to achieve effectiveness and efficiency based on the assumption that coordination through network arrangements that involves further stakeholders have more potential to deal with transnational security risks, mostly because non-state actors have the necessary resources, flexibility and experience to cope with today's complexity and reinforce the action of national governments (Hegemann and Kahl 2016). As a consequence, the making and the implementation of security policy has shift towards privatization and marketization. The complexity of new threats, the limited capacities of states and the provision of security based on cost-efficient guidelines requires new forms of cooperation with other actors, including other states, international organisations, non-governmental organisations and the private sector and the use of their resources and expertise to respond to these new threats - governance (Kirchner 2007, p.9; Krahmann 2005b, pp.537-538). In this scenario, the governance system does not only aim to offer a new alternative process of governing, but it is also seeking to achieve greater efficiency in the management and addressing of social and political issues (Stoker 1998).

Therefore, the exclusiveness of the state to provide security is being eroded, and the monopoly of the use of force by the state is being replaced by the need of efficiency and cost-effectiveness. This is because addressing new security threats it is not only a matter of use of force, it involves multiple resources and different actions in a time that states are not so available to invest money in the defence sector, hence the need for efficiency and cost-effectiveness (Krahmann 2005a, pp.18-19, 23).

1.3.2. Security Governance Conceptual Framework

Security governance has been identified as a heuristic device, that emerged to address the new challenges underlying the post-Cold War security landscape, namely concerning the widening and deepening of the security agenda, the emergence of new security actors and the need to reconstruct regional and global systems of security governance (Hegemann and Kahl 2016; Christou et al. 2010; Kirchner 2007). This sub-chapter aims to introduce the central discussions underlying the conceptualisation and understanding of security governance.

Security governance has been used both as a concept and as a political practice, and these usages are not inconsistent. On the one hand, it analyses the assumptions of the security landscape and describe the underlying dynamics of the making and implementation of security policy. On the other hand, it also has a normative dimension that guides political practices, meaning that political actors, as the European Union, implement elements of the security governance framework in order to achieve effective and legitimate courses of actions. Therefore, besides its descriptive and analytical framework, security governance has a prescriptive dimension by proposing guidelines for the effective and legitimate management and regulation of security risks and challenges (Hegemann and Kahl 2016; Bevir and Hall 2014; Sperling and Webber 2014).

According to Christou et al. (2010), the literature on security governance has evolved through three central waves. The first wave introduced the conceptual framework of security governance and its empirical applications in the transformed post-Cold War Euro-Atlantic security context, namely in the EU and in NATO. The second wave proceed with discussions on the refinement of the concept, the works of Webber et al. (2004) and Krahmann (2003a) are of particular relevance. Afterwards, the third wave was based on the application of the concept of security governance to the European context. Since its inception, security governance was considered as being a European specific, the third wave reinforced this idea by offering a path to understand the provision of security in Europe, namely at EU level, which was considered the perfect example of security governance, considering its multi-level arrangements. Nevertheless, the evolution of the literature on security governance was accompanied by some criticism towards the Eurocentric perspective underlying this conceptual framework. Thereof, multiple scholars started to apply the security governance analytical framework beyond the European region to other national and regional contexts, and they also started to explore alternative avenues and dialogue with more established theories of International Relations and Security Studies. Resulting in a fourth wave of scholarship that attempts to apply the concept of security governance beyond the European context, to other regions and at the global level

(Hegemann and Kahl 2016; Ehrhart, Hegemann and Kahl 2014b; Sperling and Webber 2014; Christou et al. 2010).

Despite the multiple efforts to conceptualise security governance, it has remained a contested and diffuse concept, which does not have a consensual definition. This lack of consensus is justified by the two elements that compose it, *security* and *governance*, two terms that are both contested and controversial (Hegemann and Kahl 2016; Kirchner 2006). Therefore, in order to better understand the concept of security governance it is important to clarify the underlying discussions concerning the concepts of *security* and *governance*.

In relation to the concept of *security*, it remains a contested concept both at the academic and at the political level (Christou et al. 2010, p.341). Traditionally, considering the international anarchic system of interstate actions and interactions, the security policy is designed and implemented to protect the territorial integrity and the political sovereignty of the state, the threat is mostly military as well as the means to address it. The context underlying the end of the Cold War, the consequent collapse of bipolarity and the decreasing risk of superpower confrontation, is marked by on the one hand, the decrease of likelihood of interstate war, and, on the other hand, the increasing of non-traditional threats, which are more diverse, less identifiable and less predictable, such as civil war, transnational crime, terrorism and infectious diseases (Daase and Friesendorf 2010, p.2; Kirchner 2006, p.949). As a consequence, the debate underlying the concept of security has been contested since the 1980s, with several attempts to deepen and widen the concept, deepen from the state level to also consider societies and individuals as referent objects, and widen to consider beyond the military sector, the social, the economic, the environmental and the political sectors (Christou et al. 2010; Daase and Friesendorf 2010; Kirchner 2006; Webber et al. 2004; Krahmann 2003a; Buzan, Waever and de Wilde 1998).

There are multiple perspectives on security, it can be understood in terms of power relations between states in the international anarchic system (Waltz 1979); as a socially constructed concept (Huysmans 2002; Wendt 1992); in terms of emancipation (Booth 1991). Moreover, security has also been understood as ‘freedom from fear’ or ‘freedom from want’ (UNDP 1994). At the political level, security has been instrumentalised to justify for instance invasions, as the invasion of Iraq in 2003; to justify peacekeeping missions; to justify the existence of international organisations; and to justify the development and reform policies in states after conflict. Therefore, security has the potential to mean different things to different groups in different contexts and at different times (Christou et al. 2010, pp.341,343).

Therefore, the complexities underlying new security challenges, new actors, new instruments and new practices meant that the provision of security “came to be interpreted as a problem of governance” (Christou et al. 2010, p.343; Daase and Friesendorf 2010, p.2).

The literature on governance emerged for the first time to analyse domestic politics in the 1970s, following new modernist theories and reforms in the public sector as a reaction to the crises of the bureaucratic state (Bevir and Hall 2014, pp.22-25). Afterwards, in the early 1990s, it spilled over into the international realm, first to be applied to “soft” issues, mainly economic, and then to “harder” issues such as security and defence (Bevir and Hall 2014, p.26; Kohler-Koch and Rittberger 2006, pp. 29-30). At the international level, the emergence of governance is mainly associated with the end of the Cold War and the collapse of an ideological power struggle, and a consequent greater necessity and willingness from governments to collaborate internationally. Moreover, the process of globalisation and the international interdependence in trade, finance and technology have contributed to the emergence and/or exacerbation of new challenges. The growing pressure of the new transnational challenges exposed the limitations in terms of resources and capabilities of states to address them unilaterally (Kohler-Koch and Rittberger 2006, pp.29-30; Krahmann 2003b, pp.329-330). Therefore, the usage of the governance literature to international relations results from the emergence of new threats, new actors and the growing need to coordinate the interactions among these actors (Bevir and Hall 2014, pp.22-25).

In relation to the concept of governance, similarly to the concept of security, it has been applied differently by multiple actors at the academic and at the political level, translating into a proliferation of meanings and vagueness, and consequently into a lack of consensual definition (Sperling and Webber 2019; Christiansen 2013; Daase and Friesendorf 2010; Lake 2010; Kohler-Koch and Rittberger 2006; Krahmann 2003a; Stoker 1998; Rhodes 1996). Moreover, it has been applied to different geographic levels – local, national, regional and global – and to different topics – environment, energy, economy, cyberspace, etc. (Sperling and Webber 2014, p.126).

The academic literature on governance has been eclectic and has multiple origins and usages, such as institutional economics, political science, organisational studies, development studies, public administration (Krahmann 2003b, pp.323-324; Stoker 1998, p.18). According to Rhodes (1996), governance is used at least in six different contexts: to refer to the minimal state; to refer to corporate governance; to refer to the new public management; to refer to good governance; to refer to socio-cybernetic systems; and to refer to self-organising networks (pp.652-653). Therefore, governance has been used as a catch-all term associated with multiple scenarios (Smouts 1998, p.81). On the one hand, some authors perceive this flexibility as the secret for its widespread use, acceptance and success, whereas others see this vagueness as a problem that could undermine its utility and remove its meaning (Sperling and Webber 2014, p.126; Christiansen 2013, p.104; Kohler-Koch and Rittberger 2006, p.28; Krahmann 2003b, p.326).

In terms of the conceptualisation of governance, there have been multiple efforts. Pierre (in Kohler-Koch and Rittberger 2006) identifies two understandings: one conceptual and one procedural. As a conceptual framework, governance describes the co-ordination by multiple actors of the social systems. As a procedural, governance is a process through which public and private actors coordinate to manage and regulate social systems. Therefore, governance is both a conceptual framework that describes and analyses the co-ordination of social systems, but it also has a normative and a prescriptive dimension by being presented as a form of governmentality (pp.28-29). The concept of governance has also been framed in terms of authority relationships, the authority exercised by state at the national level, the authority exercised by international organisations over member states (supranationalism), the authority that non-governmental organisations and corporations exert over local communities (private authority) (Lake 2010). Another use is the term of 'good governance', introduced in the late 1980s by the economic development discourse, used by international financial institutions to justify political reforms imposed to countries that are recipient of loans, and was afterwards borrowed to the political sphere. In the political realm, 'good governance' is mostly associated with political systems which legitimacy results from democratic mandate, the rule of law, free market competition and increasing involvement of non-state actors (Kohler-Koch and Rittberger 2006, pp.28-29; Smouts 1998, p.81).

Despite the multiple understandings and applications of this concept there is one shared assumption that is that governance is different from government. Accordingly, whereas government refers to the hierarchical decision-making process and structures centred on the state and public actors, vertical and centralised chains of authority and the management and regulation of societies through coercion and consent; governance refers to the heterarchical decision-making process beyond state and public actors, horizontal and decentralised authority and the management and regulation of societies more by consent or an aggregation of preferences rather than coercion (Sperling and Webber 2019; Sperling and Webber 2014; Daase and Friesendorf 2010; Kirchner 2006; Kohler-Koch and Rittberger 2006; Smouts 1998; Stoker 1998).

The governance system implies the absence of a central authority and is based on the collaboration and cooperation among multiple and diverse actors. Hence, while states maintain a key role, they no longer hold an exclusive position and share responsibilities with other actors, such as international organisations, NGOs and the private sector, which play an increasing role in the formulation, implementation and monitoring of politics and responses to global issues (Krahmann 2003a; Smouts 1998; Stoker 1998; Rhodes 1996; Gordenker and Weiss 1995). Therefore, governing in a governance framework is considered to be an interacting process, since state actors alone do not have the capabilities, the resources and the knowledge to tackle challenges unilaterally, resulting in the constant contracting and building up of partnerships between public and private actors. Thus, governance involves multiple forms of partnerships: principal-agent relations, inter-organisational negotiation and systemic coordination. The management and regulation of international affairs is not exclusively based on interstate activity, but is underlined by an interactive process of constant negotiation between heterogeneous actors (Stoker 1998). Notwithstanding, Bevir, Daddow and Hall (2014) defy the novelty underlying the centrality of role of other actors beyond the state in governing political affairs. The assumption of the exclusiveness of states interacting in the international anarchic system was always considered a formal myth. Accordingly, this assumption neglected the existence of other international practices and actors beyond the state that already existed. Thus, the "new features of global governance may have spread, but they have always been there" (*ibid* p.11).

Therefore, governance is a "way of governing that does not assume the presence of a traditional, hierarchical government at the helm of the polity" (Christiansen 2013, p.103). This shift from government to governance reflects a growing fragmentation and integration of political authority among public and private actors (Krahmann 2005b). However, it is important to note that governance does not mean the absence of government, but the regulation of social and political issues drawn from, but also beyond government (Stoker 1998). Thus, the main difference between governance and government is in the process and in the scope, the nature tends to be the same. Accordingly, governance is more encompassing than government, because it considers other actors beyond the state and the importance of collective action (Smouts 1998; Stoker 1998).

Following the introduction of the main discussions on *security* and *governance*, we believe that in the absence of a clear and consensual definition of security governance, we choose to understand it from the perspective of its main characteristics. As an intentional system of governing, that involves the cooperative and coordinated management and regulation of security issues by multiple actors, public and private; that functions in the absence of a central authority, and is institutionalised through formal and informal arrangements; structured by norms, values and interdependent needs and interests, and directed towards specific particular outcomes, namely efficiency and legitimacy (Kirchner 2006, p.948; Krahmann 2005a, p.20; Webber et al. 2004, p.3). Hence, security governance comprises five core features, coordination without a central hierarchy - heterarchy; de-centralised character based on the fragmentation of political authority among multiple actors, public and private; interaction which is institutionalised formally and informally; relations that are based on shared ideas and structured by norms and inter-subjective understandings and formal regulations – voluntary compliance mechanisms; and collective purpose (Ehrhart, Hegemann and Kahl 2014a, p.146; Webber et al. 2004, p.8).

There are three main elements underlying the concept of security governance that need further clarification.

First, in the governance framework the political authority is de-centralised, meaning that there are multiple actors, public and private, involved in the management of common affairs. Thus, it assumes a detachment from a state-centric perspective to include actors such as civil society, private sector, transnational organisations, but also the state and national governments. As far as it concerns the field of security, an area that is traditionally the responsibility of the state, has also noticed a significant intervention of non-state actors in the policy-making and implementation of security policies. Nevertheless, states remain the key actors in the provision of security, considering that states are "the agents through which the structures of governance are instituted and financed, and the agents through which the efforts of these structures are largely realised" (Webber et al. 2004, pp.5-6).

Second, the interactions between these multiple actors are guided not only by interests, but also by beliefs, ideas and norms, which have a crucial role in governance. Governance, as already mentioned, is a fragmented system of governing and it is not dependent upon vertical authority as government. Hence, in order to function smoothly the governing system should be based on shared inter-subjective meanings and ideas about a desirable end state. Considering that governance is not guided by compulsion and coercion as the government system, the formal institutionalised interaction between multiple actors is dependent on the willingness to act, shared ideas, norms and values. Thus, in this context ideas matter. Accordingly, actors compete on which ideas should be projected in order to achieve particular objectives in the security area (Webber et al. 2004, pp.5-6).

Third, the arrangements and interactions underlying security governance result from the interest in maintaining collective order and achieving shared goals, through collective process of rule. Hence, it functions according a structure and a process. As far as it concerns to structure, governance is built upon institutions and the particular forms of behaviour among participants that are defined and guided by rules of entry, norms of interaction and constraints on behaviour. As far as it concerns to process, it relates to the achievement of policy outcomes and the path of interaction between participants to define and achieve them. The objectives reflect an aggregation of interests and ideas among actors, which tend to converge, but occasionally may be contested. Furthermore, some objectives can reflect the majority and not necessarily all actors (Webber et al. 2004, pp.7-8).

As previously mentioned, security governance is an analytical concept and a political practice that make normative claims about its consequence. Accordingly, certain prerequisites (shared interests and goals, and norms and ideas) and structures (multiple actors, de-centralised modes of cooperation, and voluntary compliance mechanisms) lead to effectiveness and legitimacy (Ehrhart, Hegemann and Kahl 2014a, p.148).

First, as far as it concerns to prerequisites, considering the de-centralised nature and the absence of a central and hierarchical political authority underlying the concept of security governance, coordination among multiple actors cannot be enforced from above. Consequently, it requires basic consensus on the problems and the challenges to be addressed, a cooperative approach, and shared general principles that guide common action. Thus, security governance requires common, or at least, compatible interests and goals – interdependent needs and interests - as well as shared norms and ideas – collective purpose -, otherwise actors will not engage in potentially costly governance efforts (Ehrhart, Hegemann and Kahl 2014a, pp.148-149).

Second, the structures refer to the multiple actors, modes of cooperation and compliance mechanisms underlying security governance. Accordingly, structures of security governance refer to fragmented forms of coordination among public and private actors, through formal and informal arrangements and cooperative processes and mechanisms rather that hierarchical command-and-control structures. Therefore, ideal structures of security governance should rely on "pluralistic constellations of actors, heterarchic modes of cooperation, and voluntary compliance mechanisms" (Ehrhart, Hegemann and Kahl 2014a, p.149).

Third, security governance has also a normative dimension, considering that it not only describes modes of security provision, but it prescribes specific desired consequences, by assuming that through the prerequisites and structures underlying security governance it consequently will produce effectiveness and legitimacy. Therefore, according to Ehrhart, Hegemann and Kahl (2014a), security governance "is a result of the search for more efficacious and accepted responses to transnational risks in the globalised, post-cold war order" (p.149).

1.3.3. Conceptual Framework of Securitisation

Despite the added value of the concept of security governance to the achievement of the research objectives of this study, it is limited in terms of understanding the construction of the meaning of security and how security logic emerges in the first place. Thus, the concept of security governance benefits from the incorporation of the conceptual framework of securitisation (Christou et al. 2010). This sub-chapter aims to support the understanding on how actors construct and give meaning to security threats and how these understandings translate into the development of policies, by introducing the concept of securitisation.

The concept of securitisation emerged in the framework of the debate underlying the broadening and the deepening of the concept of security in the post-Cold War context. In this scenario, in 1983, Barry Buzan introduced the assumption of different sectors of security beyond the military sector, to also consider the environmental, economic, societal and political sectors. However, this broadening is accompanied by the danger of considering everything as security, with potential intellectual and political implications for its coherence and effective meaning. Hence, the Copenhagen School, mainly through the proposals of Barry Buzan and Ole Waever, introduced the concept of securitisation as an alternative understanding of security, with the aim of suggesting an analytical framework to analyse what is and what is not a security issue and overcome the challenges posed by the debate on the broadening and deepening of the concept of security (Vuori 2017, p.65; Balzacq 2010, p.59; Peoples and Vaughan-Williams 2010, p.76; Buzan and Hansen 2009, p.212).

According to Buzan and Hansen (2009), securitisation refers to the discursive conceptualisation of security (p.212). Hence, security is a socially constructed concept through discourse, is a speech act, is a process that does something to a certain issue, rather than an objective condition. Securitisation is a performative concept that results from discursive politics (Vuori 2017, p.65; Buzan and Hansen 2009, p.212). Hence, securitisation refers to the intersubjective socio-political process of discursively framing an issue in security terms and presenting it as posing an existential threat by securitising actors to a particular referent object (Vuori 2017, p.65; Balzacq 2010, p.59; Emmers 2010, p.137; Buzan and Hansen 2009, p.212). Accordingly, 'saying it is doing it', by saying certain words we also perform a particular action.

Thus, by discursively framing the security status of an issue the securitising actor claims a right to use exceptional means to address it (Peoples and Vaughan-Williams 2010, p.77).

The securitising actor refers to an actor that is in a position of authority and has social and political capital that enables it to convince an audience of the existential threat posed to a particular referent object. In principle, anyone is entitled to proceed with the securitising move. Nevertheless, in practice, there are actors that are more successful and have privileged positions, that have more credibility with the relevant audience, and common than others in the securitisation process, as is the case with governments, political leaders, the military, lobbyists and pressure groups (Emmers 2010, p.139; Peoples and Vaughan-Williams 2010, p.79; Buzan and Hansen 2009, p.212).

The process of securitisation has two main phases. Firstly, a politicised issue, an issue that is addressed, managed and regulated within regular political procedures, is articulated by securitising actors in security terms and as an existential threat to a certain referent object. In this scenario, a particular issue, person, entity or phenomena is depicted as posing a threat to the survival of the referent object, which can take many forms, from the State, national sovereignty, ideology, economy, collective identities, species up to habitats (Emmers 2010, p.139). Nevertheless, it is important to note that certain objects have more potential to be securitise if associated for instance with historical connotations of threat, danger and harm (Peoples and Vaughan-Williams 2010, p.79). The securitising actor claims a sense of urgency, that an issue should be treated with priority, and the need to adopt exceptional measures beyond standard political procedures. On the one hand, the articulation of urgency and exceptional measures sets the boundary between what is to be consider as 'security proper' (Buzan and Hansen 2009, pp.215-216). However, on the other hand, there is a potential danger in this sense of urgency and exceptionality of unintended consequences and also the process can be a way to legitimise and empower the military in civilian activities and in granting governments the legal framework for suspending civil and liberal rights (Emmers 2010, p.142; Buzan and Hansen 2009, p.217).

Secondly, however, the adoption of measures is not a requirement, the securitising actor can succeed in securitising an issue without implementing extraordinary measures and proceed with regular public policy procedures. But, to complete the process of securitisation the securitising actor has to succeed in the second phase of convicting a relevant audience of the existential nature of the threat to the referent object. Hence, the securitising move is successfully completed when a relevant audience – public opinion, politicians, military or other elites – is convinced and accept the urgency in adopting extraordinary measures to address an existential threat posed to a referent object (Emmers 2010, pp.139,141).

Therefore, in these terms' security is socially constructed as a speech act, meaning that a particular statement do more than describe realities, it has specific implications in the action realm. They are performative, the successful articulation of an issue in security terms, translates into concrete measures and procedures, usually urgent and exceptional measures (Emmers 2010, p.139).

1.3.4. Fighting Online Disinformation: Confronting, Blocking, Naturalising and/or Ignoring?

This sub-chapter introduces the four ideal-type analytical model proposed by Hellman and Wagnsson (2017) with the aim of supporting the achievement of the research goals of this study particularly the analysis of the strategic considerations underlying the moral authority of the security governance of online disinformation by the European Union. The strategic considerations underlying the concept of moral authority, which will be further discussed in the next sub-chapter, refers to level of reaction to a particular issue. The adoption of this model seeks to inform the strategic considerations by characterising the response to the challenge of online disinformation at EU level.

According to Tenove (2020, p.524), addressing disinformation as a security threat is often appropriate, considering its potential to undermine the ability of citizens to enact in democratic life. Moreover, security agencies, through for instance intelligence, are better prepare to collect information about the source and support a more effective response. Nevertheless, on the one hand, these security organisms have complicated relation with democracy, because they tend to be under weak democratic control and can contribute to excessive influence in the democratic process by the incumbent government. On the other hand, the use of security laws against disinformation in authoritarian countries is well-documented, but there are also emerging concerns that some democracies have been employing policies that can contradict democratic principles such as the freedom of expression (Tenove 2020). Therefore, there is an urgent need to assess how democracies, in this case how the European Union has been addressing the issue of online disinformation as a threat. For this purpose, we use the four ideal-type analytical model – confronting, blocking, naturalising and ignoring – proposed by Hellman and Wagnsson (2017).

According to the model proposed by Hellman and Wagnsson (2017), the Member States of the EU can employ a more engaging response, through confronting or blocking, or a more disengaging response, through naturalising or ignoring. The engaging approach envisages a more offensive posture, that actively confronts the perceived external adversarial narratives[6]. The disengaging approach reflects a more defensive posture, a narrative is created and disseminated, but it is not directed towards a particular external adversarial narrative.

The confronting approach is based on an outward-looking strategy. The focus is to actively produce and project counter-narratives, usually in direct response to a particular external adversarial narrative that is perceived as fake, imprecise and that denigrates. Therefore, particular events are refuted or reinterpreted, through the presentation of empirical evidence and sources that are considered and represented as trustworthy. This model represents the most hostile and antagonistic strategy, which in turn can contradict a pluralistic and democratic system (Hellman and Wagnsson 2017, pp.158-159).

The blocking approach is based on an inward-looking approach. The focus is to protect the national strategic narrative without directly producing and projecting a counter-narrative, but by blocking external adversarial narratives. This strategy is constituted by measures and restrictions that aim at controlling and blocking selectively information, thus denying public access to the narrative projected by the 'other'. Therefore, this strategy manifests symptoms of non-democratic and authoritarian regimes, colliding with democratic values. Furthermore, technological evolution enables alternatives to promote content, thus undermining the success and effectiveness of this strategy (Hellman and Wagnsson 2017, pp.161-162).

The naturalising approach is outward-looking and its objective is to produce and project strategic narratives to external audiences. Despite the similarities with confronting, this model is less engaging, considering that the production and projection of narratives does not seek to directly oppose or contradict external narratives, just to project a positive and appealing image of its own and ignore the other. Therefore, the goal of this strategy is to win trust of the audience by its own strategic narratives, and not through opposite counter-narratives. Openness and transparency are considered the best recipe, thus this strategy is more aligned with democratic principles (Hellman and Wagnsson 2017, pp.159-161).

The ignoring approach is inward-looking, focus on the protection of its own narrative at the domestic level, without engaging with external narratives. This strategy is based on trust in

[6] For a better understanding of the concept of 'strategic narratives' see, for example, Miskimmon, O'Loughlin and Roselle (2015).

democratic institutions and in its capacity to defend and protect an honest, open and fair society. Hence, this strategy involves measures to actively reinforce the civil society, such as training citizens to critically assess information. Little or no attention is given to the construction of a coherent national strategic narrative, which tends to be multi-diverse and non-coherent. Nevertheless, despite its coherence with democratic values, this strategy can be unrealistic, considering its dependency on trust and on the ability of citizens to critically assess narratives (Hellman and Wagnsson 2017, pp.162-163).

In this scenario, the strategically usage of one or the combination of more than one model will favour the construction of a certain strategic narrative, which can contribute to the reinforcement or dissolution of conflict situations. Therefore, confronting tends to promote strategic narratives that lie on dichotomy, on 'othering', creating a division between 'us' versus the 'other', having the potential to generate conflict situations. Naturalising and ignoring tend to be less conflictual (Hellman and Wagnsson 2017, pp.164-167). According to Hellman and Wagnsson (2017, pp.164-167), the strategy that is better compatible with democracy is ignoring, considering that it allows the free flow of ideas, nevertheless unrealistic. The less compatible is blocking, considering its potential incompatibility with fundamental rights and freedoms, such as the freedom of expression.

1.3.5. Fighting Online Disinformation with Moral Authority

Despite the debatable effects and impact, online disinformation has been identified as a threat and governments and international organisations have come to recognise the need to fight it. However, the development and implementation of an effective strategy *per se* is challenging. Moreover, for democratic governments and international organisations in particular fighting disinformation is accompanied by an ethical dilemma based on the danger of losing moral ground and jeopardising democratic values and principles (Wigell 2021; Althuis and Strand 2018; Bjola 2018).

To analyse the response of the European Union to online disinformation this study uses the analytical frameworks of security governance and securitisation as well as an analytical model proposed by Hellman and Wagnsson (2017), as already introduced. Yet, they are not sufficient to evaluate the impact that the response to online disinformation at EU level has on the realisation of fundamental democratic values and principles. Thus, this sub-chapter introduces the concept of moral authority proposed by Bjola (2018) as a way to surpass the ethical dilemma underlying the response to online disinformation particularly by liberal democracies, of effectively responding without hampering fundamental rights and freedoms.

In this study we use moral authority as a framework of analysis to identify "conceptual considerations to guide and justify possible responses to digital propaganda" (Bjola 2018, p.307) and is based on two interrelated considerations, one normative and one strategic. The normative consideration refers to the evaluation of the nature of the harm, in order to justify the moral ground to engage in counter-action. The strategic consideration refers to level of reaction and its relation to moral authority. Hence, the normative consideration justifies the need to respond and also informs the strategic consideration (Bjola 2018, p.307).

Therefore, we use moral authority as a framework of analysis to understand how the European Union normatively justifies its respond against online disinformation and at the same time how the European Union defines its strategy to respond and the level of proportionality underlying it.

In order to evaluate the moral ground underlying the response to online disinformation, three conceptual considerations should be taken into account: "(1) whether the actor has been harmed as a result of disinformation, (2) whether the actor has standing to engage in counter-intervention, and (3) whether the actor's reaction is appropriate in light of contextual circumstances" (Bjola 2018, p.307). Therefore, by analysing if the European Union can "make the case that it has been harmed, that it has normative standing to engage in counter-interventions, and that it does so in an appropriate manner" (Bjola 2018, p.306), this study aims to assess the moral ground underlying the response to the threat of online disinformation at EU level and thus the compatibility with the protection and promotion of democratic principles and values and fundamental rights and freedoms.

The first consideration refers to the analysis underling how the actor frames the reason to fight online disinformation. Thus, it aims to understand "why should disinformation be confronted in the first place and, relatedly, under what conditions should it be done?" (Bjola 2018, pp.307-308). In this context, despite the potential for online disinformation to cause damage, the definition and extension of harm in this case is debatable, moreover the issue of attribution is challenging. Thus, to support the moral ground defined to justify counter-actions Bjola (2018) proposes truthfulness and prudence when addressing the challenge of online disinformation.

The second consideration refers to the analysis underlying the normative standing of the actor to address the threat of online disinformation. Thus, it aims to understand "who has the right authority to address digital disinformation and why?" (Bjola 2018, p.309). The normative standing of the actor to respond to online disinformation should consider three normative attributes, accountability, integrity and effectiveness. Thus, having a normative standing to respond to online disinformation means making itself available to be public scrutinised, demonstrate consistency between objectives and actions and capacity to combat online disinformation (Bjola 2018, p.310).

The third consideration refers to the level of reaction and the ethical implications underlying the initiatives and the instruments to fight online disinformation. In this context, a source of moral authority concerning the proportional combat of disinformation is responsibility, meaning that the fighting should be conducted in a balanced manner that considers the contextual conditions and the likely nature of the harm generated (Bjola 2018, p.312).

Therefore, in order to respond to the threat of online disinformation on a moral ground, the actor should consider three sources of moral authority. First, the actor must be able to demonstrate that it has been harmed, second that it has a normative standing to respond to disinformation – is scrutinable, is consistent in terms of coherence between its objectives and its actions, and has capacity to respond - and third that its response is guided by proportionality and responsibility (Bjola 2018, p.313).

1.4. Methodological Framework

This sub-chapter introduces and justifies the methodological considerations underlying this study.

In this study, we methodologically choose a qualitative approach and use discourse analysis as method of interpretation and analysis in order to understand how the principle of proportionality is taken into consideration by the European Union in its security governance of online disinformation.

The selection of the European Union is intentional and related to the research objectives of this study, because it can provide useful insights concerning the designing and implementation of measures to address this complex security issue, especially as it concerns the consideration of the principle of proportionality in the response equation for three main reasons.

Firstly, Jakobsen (2019) argues that the European Union has become a central and an indispensable European security actor when it comes to the response to non-military threats such as disinformation, cyber-attacks and attempts to influence elections. Accordingly, these challenges demand a response that states unilaterally cannot deliver, the Union emerges as the only actor with capabilities to tackle these threats in a comprehensive and coordinated manner. This has been reflected in the initiatives set up at the EU level to counter these non-military threats challenging the contemporary European security (p.169). The case of online disinformation is particularly interesting, because the European Union already identified in the past the challenges associated with disinformation, but just now it introduced and addressed as a security issue. Therefore, it is of particular interest to understand why and how has the EU now constructed disinformation in security terms.

Secondly, the comprehensive approach of the EU to this challenge based on democratic resilience and involving awareness and media literacy programs, fact-checking initiatives, cooperation with the private sector can offer an interesting and abundant case for analysis. In this respect, we specifically highlight the relevance of the EU Code of Practice, an important initiative in terms of the cooperation with the private sector, because of its potential to contribute to the realisation of the concerns relating to the privatisation of censorship (Monti 2021) and thus associated with the challenge of responding without jeopardizing fundamental rights and freedoms.

Thirdly, the legal framework of the European Union is particularly suitable for the research objectives of this study. Proportionality is one of the core general principles of EU law (Article 5 of the Treaty on European Union) that guides de policy-making and action at EU level. In addition, despite the existence of the principle of proportionality, its implementation in this context is challenging, according to Pollicino (cited in Monti 2021, p.218) "the real challenge in Europe is not then – as in the US - if the issue of fake news can be tackled legally, but rather how this can be done in order to avoid disproportionate restriction on the fundamental rights at stake, above all the freedom of expression".

This research uses discourse analysis to evaluate the consideration of the principle of proportionality in the policy-making of the EU concerning the response to online disinformation as a threat.

The selection of this method is intentional and useful for the objectives of this research considering that we want to understand, firstly, through the conceptual framework of securitisation, how the European Union discursively constructs online disinformation in security terms, and also, how this translates into an approach of security governance that considers multiple actors and structures. Therefore, the social constructionist discourse analysis is particularly useful because it understands that "language…is not merely a channel through which information about underlying mental states and behaviour or facts about the world are communicated…is [also] a 'machine that generates, and as a result constitutes, the social world" and that “different discourses…point to different courses of action” (Jorgensen and Phillips 2002, p.9). Accordingly, in order to understand how the EU constructs online disinformation in security terms and what implications it has for the policy-making process we use the analytical framework for discourse analysis proposed by Fairclough, namely the text analysis and the social practice dimensions. The text analysis refers to the analysis of the text and its linguist characteristics to identify how discourses, namely “online disinformation as a security threat” are activated textually in the official documents of the European Union. We also want to understand how the discursive construction of online disinformation in security terms at EU level is translated into which policies, i.e. into social practice, considering that “discourse refers to language use as a social practice” (Jorgensen and Phillips 2002, p.66, 83).

Secondly, we want to understand how the European Union takes into consideration the principle of proportionality in the response to online disinformation, which is related with the competition between the interests of tackling disinformation and protecting freedom of expression. To this end, we find it useful to use the combination proposed by Jorgensen and Phillips (2002) of ‘order of discourse’ and the concepts of ‘antagonisms’ and ‘hegemony’ underlying the discourse theory proposed by Ernesto Laclau and Chantal Mouffe. In terms of ‘order of discourse’ it “denotes two or more discourses each of which strives to establish itself in the same domain…a potential or actual area of discursive conflict” (Jorgensen and Phillips 2002, p.56). The concept of ‘antagonism’, which refers to the “open conflict between different discourses in a particular order of discourse” and ‘hegemony’ that refers to “the dissolution of the conflict through a displacement of the boundaries between the discourses” (Jorgensen and Phillips 2002, p.56), to evaluate which of the discourses has hegemony at EU level. In this context, we are analysing the discursive conflict between the need for “urgent and immediate action to protect the Union, its institutions and its citizens against disinformation” versus “freedom of expression is a core value of the European Union” (European Commission and High Representative 2018a).

In relation to the sources and data collection, this study collects data through the collection of documents, particularly primary sources that are official political documents of the EU underlying the response to online disinformation as a threat. The response to online disinformation is based on ‘whole-of-society’ approach, that involves not only the Institutions of the European Union and the Member States, but actors such as civil society, journalists, fact-checkers, researchers and online platforms. Hence, the selection of official political documents considers documents that directly refer to the threat of online disinformation, but also documents that refer to other elements that are indirectly involved in the response to disinfomation.

Author	**Title**	**Type**	**Year**
Commission of the European Communities	Wider Europe – Neighborhood: A New Framework for Relations with our Eastern and Southern Neighbours	Policy Document	2003
Commission of the European Communities	European Governance: A White Paper	Policy Document	2001
Council of the European Union	Conclusions on Security and Defence	Policy Document	2021
Council of the European Union	Conclusions on the EU's Cybersecurity Strategy for the Digital Decade	Policy Document	2021
Council of the European Union	Conclusions on media literacy in an ever-changing world	Policy Document	2020
Council of the European Union	Conclusions on the strengthening of European content in the digital economy	Policy Document	2018
Council of the European Union	Conclusions on strengthening European Union-Ukraine Cooperation on Internal Security	Policy Document	2017
Council of the European Union	Conclusions on developing media literacy and critical thinking through	Policy Document	2016

	education and training		
Council of the European Union	European Security Strategy	Policy Document	2003
European Commission	2030 Digital Compass: the European way for the Digital Decade	Policy Document	2021
European Commission	Guidance on Strengthening the Code of Practice on Disinformation	Policy Document	2021
European Commission	European Democracy Action Plan	Policy Document	2020
European Commission	EU Security Union Strategy	Policy Document	2020
European Commission	Shaping Europe's digital future	Policy Document	2020
European Commission	Assessment of the Code of Practice on Disinformation	Working Document	2020
European Commission	Tackling Online Disinformation – a European Approach	Policy Document	2018
European Commission	Securing free and fair European elections	Policy Document	2018
European Commission	The European Agenda on Security	Policy Document	2015
European Commission and High	EU's Cybersecurity Strategy for the Digital Decade	Policy Document	2020

Representative/Vice-President (HR/VP)			
European Commission and High Representative/Vice-President (HR/VP)	EU Action Plan on Human Rights and Democracy	Policy Document	2020
European Commission and High Representative/Vice-President (HR/VP)	Tackling COVID-19 disinformation – Getting the facts right	Policy Document	2020
European Commission and High Representative/Vice-President (HR/VP)	Action Plan against Disinformation	Policy Document	2018
European Commission and High Representative/Vice-President (HR/VP)	Increasing resilience and bolstering capabilities to address hybrid threats	Policy Document	2018
European Commission and High Representative/Vice-President (HR/VP)	Joint Framework on countering hybrid threats – a European Union response	Policy Document	2016
European Commission and High Representative/Vice-President (HR/VP)	Action Plan on Human Rights and Democracy	Policy Document	2015

European Council	Conclusions	Policy Document	October 2020; March 2019; June 2018; June 2017; October 2017; March 2015
European Council and Council of the European Union	EU restrictive measures against Russia over Ukraine	Website	2022
European Parliament	EU strategic communication to counteract propaganda against it by third parties	Resolution	2016
European Union	The Strengthened Code of Practice on Disinformation	Policy Document	2022
European Union	A Strategic Compass for Security and Defence	Policy Document	2022
European Union	A Global Strategy for the European Union's Foreign and Security Policy	Policy Document	2016
European Union	Code of Practice on Disinformation	Policy Document	2018
European Union	Treaty on European Union and the Treaty on the Functioning of the European Union	Treaty	2009
High Representative/Vice-President (HR/VP)	Action Plan on Strategic Communication	Policy Document	2015

Table 1 – Official documments analysed

The study covers the period between 2015 and 2022, when considerable shifts and events occurred. In 2015, the threat of disinformation and the need to address it was for the first time acknowledge by the European Union. According to Hedling (2021), the concern with disinformation in EU politics it is not new, “because of the complexity of EU policy-making and its relative distance from EU citizens…politicians often misinform citizens about the EU” (p.846). Nevertheless, it was only in 2015, following the use of disinformation campaigns by Russia, that the recognition of disinformation as a threat and the need to address it accordingly took place at the EU level. Moreover, it goes until 2022 to also consider the implications of COVID-19 pandemic crisis on the response to online disinformation.

CHAPTER 2

Online Disinformation as a security threat

The objective of this chapter is to understand the construction of online disinformation in security terms, particularly considering that it is not a novel phenomenon neither in domestic nor in international politics, but the current political, economic, social and, perhaps most significantly, the technological context has enabled a more efficient and easier proliferation of these campaigns, with implications for the European security landscape. Despite its debatable effects' disinformation has been addressed as a priority in the political agendas of states and international organisations. Notwithstanding, the conceptualisation of disinformation has been contested and there is lack of clarity in the political and in the academic realm concerning what actually means for disinformation to be a security threat.

Therefore, this chapter has two core objectives. Firstly, it aims to understand the discussions underlying the conceptualisation of disinformation and the elements that contribute for the dissemination of this type of information. Subsequently, it aims to understand the discussions underlying the construction of online disinformation as a threat, particularly to democracies.

2.1. Disinformation and the Digital Era

In order to understand the conceptualisation of disinformation in the digital era, this sub-chapter has two central objectives. On the one hand, it aims to understand the definition of disinformation within the umbrella of fake news, as a type of fake news genre, through the analysis of the underlying debates on the conceptualisation of fake news. On the other hand, it aims to understand the factors that have been feeding its widespread dissemination, in order to understand what elements may be contributing to the successful proliferation of this challenge and thus threaten democracies.

2.1.1. Disinformation within the umbrella of Fake News

Although disinformation has been prominent on the political agendas of states and international organisations, in particular following the 2016 presidential elections in the United States and the 2016 United Kingdom's referendum on withdrawing from the EU in particular[7], this is not a novel phenomenon[8] (Jankowski 2018; Posetti and Matthews 2018; Roozenbeek and van der Linden 2018; Tandoc Jr., Lim and Ling 2018; Brennen 2017). Nevertheless, this does not translate into a universal definition. This study understands disinformation as a type of fake news and to better understand the conceptualisation of disinformation itself, this sub-chapter starts by presenting first the underlying debates concerning the conceptualisation of fake news.

In the academic debate, traditionally, fake news has been mostly understood as similar to satire (Monsees 2020, p.2; Egelhofer and Lecheler 2019, p.97; Mourão and Robertson 2019, p.3; Tandoc Jr., Lim and Ling 2018, p.141). However, on the one hand, the term became elastic and has been applied to describe multiple activities (Bakir and McStay 2017, p.1; McGonagle 2017, p.204), contributing to a muddy definition (Mourão and Robertson 2019, p.1; Waisbord 2018, p.1866). Consequently, Farkas and Schou (cited in Jankwoski 2018, p.251) argue that fake news has no definition and it is useless to try to determine its exact meaning. On the other hand, fake news has also been perceived, particularly by traditional media, as a problematic and inappropriate term that shouldn't be used. Accordingly, fake news has been understood by some authors as an oxymoron, a contradiction, and its usage contributes to the normalisation of its appropriation by political actors to discredit and attack traditional media (Wardle and Derakhshan 2018, p.45).

The absence of a clear definition of fake news can be problematic and dangerous, because the variation of the term and the preoccupation with a particular sub-set of fake news, namely with disinformation, should not inform a broader legal framework. The arbitrary interpretation of the term has the potential to translate into the formulation and implementation of fragile and inappropriate strategies to address this phenomenon, and also into a disproportionate legal framework (McGonagle 2017, p.204). Moreover, fake news and disinformation often appears blended with hate speech, which is illegal content, further challenging the response to this type of content (la Cour 2020, p.709).

Notwithstanding, multiple efforts have been made in order to define and operationalise the term 'fake news', which can be organised in three main groups: definition through categorisation; relational definition; and two-phenomenon definition.

[7] For a detailed understanding on the debate concerning disinformation in the context of 2016 US presidential elections and Brexit referendum see, for instance, Guess, Nagler and Tucker (2019), Mourão and Robertson (2019), Bennett and Livingston (2018) and Jankowski (2018).

[8] It is difficult to accurately identify the origins of fake news (Jankowski 2018, p.248), but for a detailed understanding of its historical evolution see, for instance, Posetti and Matthews (2018), Darnton (2017), and Hirst (2017).

First, the literature has defined fake news through the categorisation of the forms it may acquire. Tandoc Jr, Lim and Ling (2018) conceptualised the term 'fake news' through six categories based on their level of facticity and deception – satire, parody, news fabrication, photo manipulation, advertising and public relations, and propaganda[9]. Similarly, Wardle and Derakhshan (2018) also understand fake news through categories – false connection, false context, manipulated content, misleading content, impostor content, fabricated content and satire/parody[10].

Second, fake news has also been defined in relation to the concept of 'real news'. 'Real news' are understood as being the output of journalism, produced in accordance with the western journalistic normative model, hence, they must be objective, factual, independent, trustworthy, accurate and informing. Fake news contradicts this model, thus they are the opposite of 'real news' (Mourão and Robertson 2019, p.14; Berger 2018, p.7). Notwithstanding, this understanding can be highly problematic. On the one hand, despite the responsibility of the journalist to produce neutral, trustworthy and accurate content, news are socially constructed. Therefore, journalists are subject to individual subjective judgments and external forces, such as the competition for audiences (Tandoc Jr. Lim and Ling 2018, p.14). Moreover, Mourão and Robertson (2019, p.4) argue about the perils of defining fake news in opposition to 'real news' as conceptualised by the western normative model. Classifying everything that is not in accordance with the western normative model as fake news can ignore alternative forms of doing journalism and take ethnocentric connotations.

Third, fake news has also been understood as a two-dimensional phenomenon (Egelhofer and Lecheler 2019, p.97; Monsees 2018, p.2). According to Egelhofer and Lecheler (2019, p.97), fake news is a two-dimensional phenomenon of public communication divided into categories of fake news genre and fake news label.

The fake news genre is the dimension that has gained more attention at the governmental level and in the academic debate. The literature identifies three main characteristics that must be fulfilled in order to consider something as fake news (Egelhofer and Lecheler 2019, p.97; Mourão and Robertson 2019, p.3; Jankowski 2018, p.248; McManus and Michaud 2018, p.19; Waisbord 2018, p.1866; McGonagle 2017, p.203).

Firstly, fake news tends to be low in facticity and contains false information. Nevertheless, as Mourão and Robertson (2019, pp.3-4) claim, falsehood can exist in a continuum, thus the

[9] For a detailed understating see Tandoc Jr., Lim and Ling (2018).

[10] For a detailed understating see Wardle and Derakhshan (2018).

presence of facts does not disqualify something as fake news. The content can be completely fabricated, partly untrue or it can have elements of truth, but be misleading, making content more believable and resilient. Therefore, the relation between fake news and falsehood is not straightforward, and has the potential to generate a problematic debate on who is entitled to define the dividing line between truth and falsehood (Hirst 2017, p.82).

In this scenario, Wardle and Derakhshan (2018) identify three types of information that often overlap and demonstrate the porosity underlying the delimitations of falsehood in the concept of fake news: misinformation, disinformation and malinformation. Misinformation refers to the unintentional publication of false or misleading information. Disinformation refers to the strategic intentional publication of false or misleading information. Malinformation refers to the publication of factual and accurate information to cause harm.

Secondly, fake news mimics the format of traditional media (headline, text body, picture and, in the case of online fake news, the URL) and appropriates the techniques of journalism (Egelhofer and Lecheler 2019, p.100; Jankowski 2018, p.248; Tandoc Jr, Lim and Ling 2018, p.147; Waisbord 2018, p.1866; Brennen 2017, p.180; McGonagle 2017, p.204). This appropriation seeks to grant legitimacy, credibility and trustworthiness to the content, by giving a false sense that it resulted from journalistic research and obeys certain normative standards (Egelhofer and Lecheler 2019, p.100; Tandoc Jr, Lim and Ling 2018, p.148; Bakir and McStay 2017, p.4).

Thirdly, fake news is intentional and is produced with the intention of deceiving, which is considered the “defining element of fake news” (Egelhofer and Lecheler 2019, p.100; Mourão and Robertson 2019, p.3; Humprecht 2018, p.3; Jankowski 2018, p.248; Morgan 2018, pp.39-40; Tandoc Jr, Lim and Ling 2018, p.138; McGonagle 2017, p.203). Fake news intentionally produced and disseminated through digital platforms[11] may seek to generate profits – economic motivation - or to achieve political goals – political motivation (Humprecht, Esser and Aelst 2020, p.494). On the one hand, sensationalist stories become viral and therefore profitable, because their titles are usually appealing and attract users to click, which then converts into revenues (Allcott and Gentzkow 2017, p.217). Hence, the algorithm-driven mechanisms of social media have been used to manipulate emotions and generate attention in order to convert it into advertising revenue - ‘economy of emotions’ (Bakir and McStay 2017). On the other

[11] According to Hirst (2017) fake news has been narrowly represented as technological phenomenon, and its production and dissemination through traditional print and broadcast channels have been neglected. However, for the purposes of this research we focus on the production and dissemination of fake news in the online environment.

hand, the political motivation lies in the intention to manipulate the minds, to influence the opinion and behaviour of citizens concerning critical political issues, in order to achieve strategic objectives. In this scenario, different from other types of influence activities, the use of fake news genre has at is core the aim to disrupt, divide and confuse, to destroy existent cohesive narratives rather than replace them (la Cour 2020, p.711; Berger 2018, p.10; Haiden 2018, p.8; Humprecht 2018, p.3; Morgan 2018, pp.39-40; Tandoc Jr, Lim and Ling 2018, p.138).

Therefore, the fake news genre refers to the "deliberate creation of pseudojournalistic disinformation" (Egelhofer and Lecheler 2019, p.97). Disinformation, similar to fake news, is not a novelty, but it lacks universal definition and has been confused with other concepts, such as 'propaganda', 'influence operations', 'information operations' and 'information war'[12] (Egelhofer and Lecheler 2019, pp.101-102; Humprecht 2018, p.2). Moreover, it has also been understood in terms of a single disinformation story, a disinformation campaign or disinformation operation (la Cour 2020, p.705). Nevertheless, for the purposes of this study, we understand disinformation as a type of information[13][14] that is false or misleading, intentionally created and disseminated by state and non-state actors, namely to deceive and confuse, to influence the political process of the target and disrupt normal democratic order, in order to achieve strategic objectives in international politics (Egelhofer and Lecheler 2019, pp.101-102; Gioe, Goodman and Wanless 2019, p.123; Lanoszka 2019, p.229; Bennett and Livingston 2018, p.122; Berger 2018, p.7; Gerrits 2018, pp.4-5; Humprecht 2018, pp.2-3; Tandoc Jr., Lim and Ling 2018, p.140; Wardle and Derakhshan 2018, pp.45-46).

Notwithstanding, fake news is not limited to a particular actor, context[15], country or political system (Gerrits 2018, p.7), it has been employed by state and non-state actors (Waisbord 2018, p.1867), in peace and conflict situations (Clements 2014, p.217), domestically and internationally, in democratic and authoritarian regimes (McGonagle 2017, pp.203, 205).

[12] According to Gioe, Goodman and Wanless (2019, p.123), there are many terms to describe the deliberate manipulation of information for strategic aims, which can explain the lack of universal definition of disinformation and the confusion with other terms. To a detailed understanding of these concepts and the underlying differences see, for instance, Wanless and Pamment (2019).

[13] Nevertheless, according to Floridi (cited in Fallis 2011, p.202), information is based on truthful data, thus to consider something as information it must be true. Hence, false information is a contradiction in terms. Therefore, disinformation is not a type of information if it is false. Notwithstanding, as Fallis (2011, p.203), we share the assumption that any data should be considered as information, be it true or false. Moreover, producing and disseminating false information is also information considering that it says at least something about who produces it.

[14] Information can be presented in the form of text, images, video and audio (Fallis 2011, p.208).

[15] It is important to note that disinformation is also shaped by national information environments, it tends to mirror the national political agendas, see, for example, Humprecht (2018).

Moreover, it has the potential to affect different targets, from soldiers on a mission, the general public to key-decision makers (la Cour 2020, p.708). Therefore, disinformation is type of false or manipulated information intentionally produced, but it may arise in many shapes and forms, and may be produced and disseminated by a variety of actors with different purposes, whose targets may also vary. Hence, the perpetrators may vary from individuals trying to make a profit from click-bait, as was the case of the group of Macedonian teenagers that earned millions of dollars by producing fake news on social media during the 2016 U.S. presidential election campaign, to a state actor seeking to influence public debate in other countries (la Cour 2020, p.708). Nevertheless, the empirical delimitation of these realities is not straightforward. Large volumes of independently produced false or manipulated information for economic gains often uses political aspects that are afterwards instrumentalised and distributed as part of a larger political disinformation campaign (Bennett and Livingston 2018, pp.127-128). Consequently, according to Monsees (2020, p.3), economic incentives contribute to the ease of the spread of political disinformation.

The term fake news has also been instrumentalised and used as a political device in contemporary political struggles in order to delegitimise political opponents – fake news label (Monsees 2020; Egelhofer and Lecheler 2019; Farkas and Schou 2018). Therefore, labelling something as 'fake news' is also a distinct articulation of discourse, considering that it "raises the stake since fake news is by now a strong tool to denounce certain actors and messages" (Monsees 2020, pp.2-3; Monsees 2018, p.3).

In this context, Farkas and Schou (2018) conceptualise fake news as a floating signifier, a term "used by fundamentally different and in many ways deeply opposing political projects as a means of constructing political identities, conflicts and antagonisms" (p.300). Consequently, according to Farkas and Schou (2018), fake news has been articulated in three ways within broader political struggles. Firstly, fake news has been articulated as an outcome of digital capitalism, highly linked to the economic motivations previously mentioned. Hence, on the one hand, digital media technologies generate revenue according to the amount of viewers and engagement. On the other hand, research has been demonstrating that fake news generates more engagement, and its production is more profitable, considering its lower costs and high potential revenue comparing to "real news". Therefore, fake news is perceived as part of a systemic criticism of digital capitalism and combating fake news means reshaping the capitalist incentives and economic structures, namely through the promotion of funding for public institutions (Farkas and Schou 2018, p.303; Allcott and Gentzkow 2017, p.212). Secondly, fake news has been articulated as an effect of extremist right-wing partisanship, portrayed as less critical of information and more emotional. Accordingly, tackling fake news means combating extremist right-wing media corporations and politicians (Farkas and Schou 2018, pp.305-306). Thirdly, fake news has been discursively articulated as a symptom of a deeper democratic problem, which is based on the assumption that traditional media is biased and deliberately attempts to promote liberal agendas instead of representing "the people" (Farkas and Schou 2018, pp.303-306, 308). In this scenario, fake news has been instrumentalised by political actors, who have been capturing it to discredit traditional media that contradict their positions, in order to demit critique and preclude debate (Egelhofer and Lecheler 2019, p.105; Mourão and Robertson 2019, p.3; Ireton and Posetti 2018, p.14; Jankowski 2018, p.248; McManus and Michaud 2018, p.19; Waisbord 2018, p.1867; Wardle and Derakhshan 2018, p.45). According to Egelhofer and Lecheler (2019, p.105), political actors have been weaponising the term as a strategy to undermine public trust in traditional media as an important part and influent actor in the democratic system, specially on the formation of public opinion. Moreover, these accusations are generally emotional and not accompanied by explanations concerning why is the media incorrect or biased. Hence, this instrumentalisation does not seek to critically evaluate the information shared by traditional media, but to attack its legitimacy. This is problematic, by denigrating and intimidating journalism, these attacks can increase perceptions on media bias, challenge its reputation and credibility, and thus decrease trust in the journalistic industry. Consequently, this prevents the operation of journalism and the scrutiny, and ultimately the democratic process itself (Egelhofer and Lecheler 2019, pp.105-106; McGonagle 2017, p.209). Therefore, the instrumentalisation of 'fake news' to preclude scrutiny, has justified the preference for 'disinformation' (Tenove 2020, p.519). Nevertheless, this does not mean that traditional media shouldn't be criticized and scrutinised, it is important to assess the quality of the media and to evaluate if it is fulfilling its role in democratic societies, in order to promote a healthy democratic society, but the critique should accompanied by explicit and structured argumentation (Egelhofer and Lecheler 2019, pp.106-107).

The instrumentalisation of the term 'fake news' as a political device in contemporary political struggles is highly associated to what has been termed as 'post-truth'[16]. Post-truth has been used to describe and explain the current political and social context in several countries. The term 'post' suggests that the concept that follows it has become less relevant. Thus, post-

[16] Despite its current widespread use, 'post-truth' is not a novelty, in 1830 John Abercrombie in "Inquiries Concerning the Intellectual Powers and The Investigation of Truth" tried to demonstrate the questioning of facts and Science and the use of emotions for political gain (McManus and Michaud 2018, p.16).

truth means that nowadays truth has become less relevant. Accordingly, objective facts and rational arguments are less influent in the formation of public opinion than appeals to emotion and beliefs. Nevertheless, this is not entirely correct, facts that do not support certain opinions and ideas do not matter, truth still matters, but is a particular truth, a truth that is mostly not based on scientific research and evidence, but on personal experiences and emotions. Therefore, there is a struggle between different and even opposing political projects that seek to define the meaning and conditions of what should be considered as 'fake' or 'truth'. Consequently, more than defining what is truth or false is who gets the power to do it. This scenario is reinforced by a growing scepticism in societies about science, journalism and other traditional sources of information, which is problematic and it can translate in the development of policies that do not consider facts and reality (Mourão and Robertson 2019, p.15; Farkas and Schou 2018, p.308; Haiden 2018, pp.7, 11; McManus and Michaud 2018, pp.17, 20; Roozenbeek and van der Linden 2018, pp.1-2).

Notwithstanding, according to Waisbord (2018, pp.1867-1868), labelling and normalising the current era as 'post-truth' and its underlying absolute relativism is a post-modern folly, because some researchers in academia and journalism, for instance, continue to make efforts to hold accountable governments and political actors, by assessing information and exposing evidences. Moreover, the most features of post-truth era are not novel, not only politicians always lied, but also traditional media can be biased (Crilley and Chatterje-Doody 2018, p.1; Allcott and Gentzkow 2017, p.211).

The focus of this study is on the production and proliferation of misleading information – fake news genre – to accomplish political and strategic goals. In the next section, despite our focus on the online dimension, we demonstrate that the proliferation of disinformation is a result of an assemblage of factors, technological as well as economic, social and political.

2.1.2. Proliferation of disinformation: an assemblage of technological, economic, political and psychological factors

Disinformation is not a new phenomenon, neither the influence of media technology on the communication landscape and in politics, considering the impact of print press in the 19th century and radio and television in the 20th century (Allcott and Gentzkow 2017, p.211). Nevertheless, the technological evolution, namely the emergence of digital technologies as social media, brought a new dynamic and enabled an easier, cheaper and more effective way to produce and disseminate massively content (text, images, video and audio) at a higher speed and with a global reach. Hence, enabling an easier, cheaper and more effective way to produce and disseminate disinformation (Monsees 2020, p.3; Ireton and Posetti 2018, p.15; Posetti and Matthews 2018, p.1; Waisbord 2018, p.1867; Bjola 2017, p.189; Brennen 2017, p.180; McGonagle 2017, p.206). Consequently, social media has been perceived as an alternative non-military instrument to accomplish political and strategic goals beyond the use of force (Bjola 2017, p.189).

Moreover, the technological evolution particularly in the area of artificial intelligence has the potential to place even more complex dynamics, considering its role on the production of deep fake videos (Tsaruk and Korniiets 2020, p.64). Deep fakes may present in the form of audio or video[17] that has been edited to realistically portray individuals doing or saying things that probably wouldn't say or do. The rapid evolution of this technology has the potential to ease the widespread access to these tools, which in turn can be used to reinforce the production and proliferation of disinformation. Hence, automated social media accounts – bots – will become more sophisticated at mimicking human behaviour challenging the strategies that seek to detect disinformation campaigns, making response even more difficult (Paterson and Hanley 2020, p.448).

The manipulation of information has a long history, from the Trojan Horse that enabled Greek warriors to breach into the city of Troy to the Nazi regime propaganda strategies. However, according to Lin (2019), individuals are today more vulnerable to these strategies than at any earlier point in human history. On the one hand, the evolution and proliferation of information and communication technologies influenced the increase in the volume and velocity of information available. On the other hand, the technological progress was not accompanied by an evolution of the cognitive architecture of the human mind, that remains more or less unchanged. Consequently, there is a potential that cyber-enabled information warfare and disinformation campaigns in particular provide the means to replace the pillars of logic, truth and reality with fantasy, rage and fear (Lin 2019, pp.190, 194).

Thus, this research does not have a techo-deterministic point of view on the proliferation of disinformation and recognises its assemblage character as noted by Saurwein and Spencer-Smith (2020), considering that it results from a "socio-technical mix of platform design, algorithms, human factors and political and commercial incentives" (p.820). Therefore, multiple features contribute to fertilising the ground for the diffusion of disinformation:

[17] Deep fakes can also be presented in the form of text. OpenAI, a non-profit artificial intelligence research company, designed a new language model that generates convincing, realistic and well-written text.

technological – use of new digital technologies for communication -, economic – business model of social media -, as well as political and psychological – domestic social polarisation and growing levels of distrust on democratic institutions, and human cognitive architecture (Humprecht, Esser and Aelst 2020, pp.494, 498; la Cour 2020, pp.708-709).

2.1.2.1 The business model and the technical features of social media platforms

The concept of social media tends to be understood more narrowly, as an instrument of information and communication, "a form of electronic communication and networking sites that allows users to follow and share content (text, pictures, videos, etc) and ideas within an online community" (Zeitzoff 2017, p.1971). However, we understand social media beyond an instrument of information and communication,

> Internet connected platforms and software used to collect, store, aggregate, share, process, discuss or deliver user-generated and general media content … can influence knowledge and perceptions and thereby directly or indirectly prompt behaviour as a result of social interaction within networks (Nissen 2015, p.40).

The alleged Russian interference in the 2016 U.S. presidential elections and in European referendums and elections, such as the Brexit referendum and the 2017 French presidential elections, emerged as a game changer regarding the paradigm of social media, which, during the Arab Spring, had been perceived as a positive tool. The perception of social media has changed from being a positive tool that enabled social mobilisation during the Arab Spring to becoming a negative tool used for the proliferation of hate speech, recruitment for terrorist organisations, and disinformation campaigns (Jankowski 2018, p.248; Roozenbeek and van der Linden 2018, pp.1-2; Bjola 2017, p.189). Accordingly, social media amplifies human intent, be it good or bad, it can strengthen freedom of expression and empower the powerless, but it can also be a platform through which malicious actors spread disinformation, hate speech, and recruit for terrorist organizations (Ireton 2018, p.33).

Nevertheless, the malicious and hostile use of social media are not a new phenomenon. Long before the emergence of the Islamic State, Osama bin Laden had already recognised the opportunities of modern media and used the interconnectivity of the internet for subversion and information activities (Giles 2016, p.3). In the early 2000s, terrorist organisations took advantage of social media to challenge the legitimacy and credibility of the multinational force led by the United States in Iraq and Afghanistan. In this context, terrorist organisations promoted narratives on social media to influence the population of the contributing countries in order to have them question and oppose the presence of their respective countries in those regions. The central goal of these tactics was to change the centre of gravity from the physical to the cognitive domain through the proliferation of narratives and images on social media (Nissen 2015, pp.76-80).

Social media has played a relevant role in multiple situations since its introduction to the political spectrum. In the attack of Al-Shabaab in the Westgate Mall in Nairobi, the terrorist organisation used Twitter to live-tweet the attack. Islamic State uses it to promote propaganda and to recruit, while in the Iranian Twitter Revolution between 2009 and 2010 social media was used to denounce externally the abuses carried out by the Iranian regime. Finally, in 2010, social media played a relevant role in the development of the Arab Spring, contributing as a space for freedom of expression and enabling mass mobilisation (Nissen 2015, pp.76-80).

Social media has become part of contemporary conflicts and politics and has been used by both state and non-state actors to create effects in the online as well as in the offline domain (Danyk, Maliarchuk and Briggs 2017, p.13; Zeitzoff 2017, p.1971; Nissen 2015, p.8). Multiple features – trend-mechanism, network character, bots and trolls, echo-chambers and ambiguity – and the accessibility and cost-effect gains, converted social media in a weapon of choice used to collect intelligence, psychological operations[18], offensive and defensive cyber-operations, and command and control (C2), in order to accomplish political and military objectives (Nissen 2015, pp.8-9). This study focus on psychological operations, namely on how social media has been used to prompt the spread of disinformation for political purposes.

In social media, state and non-state actors try to control and explore the trend mechanism, meaning that they create and disseminate content on these platforms and by means of algorithm-driven mechanisms they become viral and almost instantaneously spread on a global scale (Posetti and Matthews 2018, p.1; Prier 2017, pp.51-52; Lange-Ionatamishvili and Svetoka 2015, p.105). This is highly linked to the business model underlying these platforms, accordingly, the user is the product, its information and attention is sold to an advertiser or, as the Cambridge Analytica scandal demonstrated, to political actors. Thus, the algorithms of these platforms are designed to learn emotions and what keeps users engaged, the more engaging, thus the more trending and viral (Nye 2019, p.10; Walker, Mercea and Bastos 2019, pp.1533-1534).

[18] Psychological operations refer to a group of military activities aimed to influence the perceptions, emotions, motives, reasoning, and behaviour of target audiences in favour of the objectives of the attacker. Psychological operations can be carried out overtly or covertly through actions such as deception, propaganda, and subversion in order to shape, inform, influence, manipulate, mislead, expose, coerce, deter, and mobilise (Nissen 2015, p.67).

Consequently, the debate has highlighted the need to regulate these platforms, considering the lack of transparency in the definition of algorithms that guide the search results and recommendations (Morgan 2018, pp.39-40; McGonagle 2017, p.207). Notwithstanding, the regulation of these platforms is accompanied by risks, not only its effects are questionable, but also its legality has been feared as an empowerment of social media platforms and censorship (Monsees 2020, pp.5,7). Therefore, this conjuncture has created a paradoxical situation, considering that the democratisation of information, enabled by the technologic evolution, namely through the internet and social media, allowed an access to an extended number of sources, including false and manipulated ones, challenging the response to phenomena as disinformation (Berger 2018, p.9; Dooley, Moore and Averin 2018, p.40; Ireton 2018, pp.33-34).

In addition, its trust-based character, formed by a network of friends or like-minded members, makes the shared content more trustworthy and legitimate than the one presented by traditional media and governmental institutions (Lange-Ionatamishvili and Svetoka 2015, pp. 104-105).

Furthermore, bots[19] and trolls[20] are used as amplifiers to share, re-share or like content, to push a certain narrative into the mainstream, creating the illusion of a widespread acceptance of the narrative and its legitimacy, contributing to its popularity and thus becoming relevant for algorithms, generating a trend (Humprecht, Esser and Aelst 2020, p.496; Saurwein and Spencer-Smith 2020, p.825; Dooley, Moore and Averin 2018, p.37; Tandoc Jr., Ling and Lim 2018, p.143). Moreover, the absence of traditional media filters, the distribution many-to-many meaning that any user can produce and distribute content, micro-targeting[21], and the existence of echo-chambers[22] enable a deeper and emotive charged circulation of disinformation, resulting in the proliferation of highly biased content and the overrepresentation of certain groups of actors in social media (Humprecht, Esser and Aelst 2020, p.496; Posetti and Matthews 2018, p.1; Bjola 2017, p.189; Lange-Ionatamishvili and Svetoka 2015, p.105).

[19] Algorithm that produces automatically content, nevertheless not all bots are used for malicious purposes (Dooley, Moore and Averin 2018, p.37).

[20] A person that seeks to destabilise and generate chaos.

[21] These digital platforms store massive volumes of data – big data - which are used to strategically produce specialised and individualised content, and to achieve political purposes (Schia and Gjesvik 2020, pp.3-4; Cavelty 2016, p.401).

[22] Echo-chamber is a closed system based on an algorithm that selects information about the connections, historic and other information about the user and exposes the user to its already existent ideas. Therefore, reinforcing beliefs by communication and repetition, and by not exposing to different perspectives and ideas (Bakir and McStay 2017, p.7).

The proliferation of disinformation is also benefited by the ambiguity associated with cyberspace, which complicates the identification of the source and its intentionality and motivations, important to plan an appropriate and proportionate response, and to legitimise counter-actions (Gioe, Goodman and Wanless 2019, p.125; Wanless and Pamment 2019, p.4; Libicki 2017, p.56). In this scenario, arguing based *on the cui bono* logic (to whose benefit?) is not sufficient to justify and legitimise political action. The ambiguity underlying cyberspace allows that attacks that seemingly benefit certain actors may be orchestrated by others. Hence, identifying and responding to perpetrators in cyberspace is challenging, because it grants plausible deniability. Consequently, certain campaigns may never be uncovered or successfully exert influence for years before its discovery (Paterson and Hanley 2020, p.442; Cavelty 2016, p.406).

2.1.2.2 Political and individual psychological features

Domestic social polarisation[23] and the decreasing levels of citizens confidence in democratic institutions have contributed to undermine the credibility of official information. Consequently, societies are more vulnerable to being exposed, accept and share disinformation, considering that individuals tend to search for alternative sources of information, which are capitalise by actors with malicious or hostile intentions (Bennett and Livingston 2018; Haiden 2018; Humprecht 2018; Morgan 2018; Tandoc Jr., Ling and Lim 2018).

On the one hand, Allcott and Gentzkow (2017, p.215) consider that the decline on trust can be both the cause and the consequence of disinformation growing tendency. On the other hand, Bennett and Livingston (2018, p.127) argue that the decreasing levels of trust result from "growing legitimacy crisis produced by the hollowing out of centre parties…diminished electoral and policy representation....and rising power of business elites and the resilience on market solutions for social problems". Furthermore, two particular historical moments fuelled this lack of trust on political actors, traditional media and on the scientific community particularly. According to Hirst (2017), for instance in the U.S., there is a "crisis of trust in traditional news sources" (p.89) – both in government and traditional media – resulting from the invasion of Iraq in 2003 and the uncritical framing of Weapons of Mass Destruction argument as a pretext for war. Moreover, the economic crisis in late 2010 has seeded mistrust

[23] For a detailed understanding on the relation between social polarisation and disinformation see, for example, Humprecht, Esser and Aelst (2020).

in economic expertise in particular an in the expert community more broadly. Consequently, there has been a shift from rational and logical evidenced based decision-making, as foundational pillars of civilised discourse, to emotional politics, from objective facts and being correct to emotions and being sincere (la Cour 2020, pp.708-709; Lin 2019, p.194).

Nevertheless, state resilience[24] towards online disinformation varies. According to Humprecht, Esser and Aelst (2020, p.497), resilience to disinformation is associated with the fulfilment of certain conditions that promote or inhibit the influence of disinformation. Accordingly, higher resilience towards disinformation is associated with lower levels of domestic social polarisation and fragmentation; lower levels of distrust in democratic institutions and other institutions such as the scientific community; healthy media regulation and public funding for fact-checking, and education and training of citizens to the reality of disinformation. Consequently, Humprecht, Esser and Aelst (2020, p.497) identified two groups of countries with higher resilience towards online disinformation - Northern European countries and Canada - and two groups with lower level of resilience towards online disinformation - southern European countries and the U.S.

At the individual level, a growing number of individuals receive and search for information online, namely through social media, increasing the likelihood of being exposed to disinformation. In these platforms there is an explosion of information, which creates the paradox of plenty, meaning that the availability of a large volume of information is accompanied by a lower level of attention, considering that individuals are overwhelmed by information, being hard to focus (Tsaruk and Korniiets 2020, p.57; Egelhofer and Lecheler 2019, p.102; Nye 2019, p.10; Roozenbeek and van der Linden 2018, pp.1-2; Tandoc Jr., Lim and Ling 2018, pp.137-138; Bakir and McStay 2017, p.7; Bjola 2017, p.189). According to Lin (2019, pp.189,194), the proliferation of digital platforms produced a more chaotic information landscape with the potential to stimulate fast, angry, reflexive, intuitive and visceral thinking, reaction and action. Consequently, people tend to use mental shortcuts to reduce the cognitive burden created by the current chaotic information landscape, hampering a more complex, reflective and rational thinking, reaction and action.

Furthermore, individuals are more predispose to consume information, whether true or false, that confirms their pre-existing attitudes, values and beliefs – confirmation bias (Ling 2020, p.1; Humprecht 2018, p.3) and assume that the accurate perception of reality is their own

[24] For a detailed understanding of the definition of resilience in this context see Humprecht, Esser and Aelst (2020, pp.497-498).

- naïve realism. Hence, divergent or opposite information is perceived as being biased, uninformed or false. Consequently, individuals with strong confirmation bias hardly trust on fact-checkers (Humprecht, Esser and Aelst 2020, pp.495-496).

Therefore, considering the process underlying disinformation - construction, dissemination, promotion and acceptance – the acceptance and sharing of disinformation as accurate information by the audience legitimises and amplifies these campaigns (Saurwein and Spencer-Smith 2020, p.825; Mourão and Robertson 2019, p.2; Tandoc Jr., Lim and Ling 2018, p.149; Waisbord 2018, p.1867).

Consequently, media literacy and raising awareness through instruments to assess information have been identified has core approaches to tackle disinformation (Humprecht 2018, pp.12-13; Ireton 2018, p.34). This has been accompanied by fact-checking activities and journalism, based on the need to identify, debunk and correct disinformation and errors. Notwithstanding, according to Crilley and Chatterje-Doody (2018, p.2), studies have demonstrated that these activities not only have had limited success, but they can also perpetuate the dissemination of falsehoods. This assumption is shared by Vargo, Guo and Amazeen (2018, pp.2029,2044), on the one hand, journalists have little ability to proactively fight fake news. Journalism is facing several challenges, namely limited time, funding and staff available, but also limited viewers, thus corrections do not spread as widely and faster as fake news. Moreover, partisan media, particularly in extremely polarised environment, can be susceptible to the influence of disinformation and be an amplifier of certain political agendas (Saurwein and Spencer-Smith 2020, p.831). On the other hand, the reactive effort of traditional media to tackle disinformation through fact-checking has not only divert resources – namely time and attention - to publish accurate news, but it also may be amplifying and contributing to the agenda-setting power of fake news. Moreover, according to Vargo, Guo and Amazeen (2018, p.2033), contemporary journalism is more focused on determining if a certain claim is factually accurate than eliminating errors or falsehoods from reporting. In addition, these activities have also disregard "how certain representations underlying the production of knowledge and identities and how these representations make various courses of action possible" (Crilley and Chatterje-Doody 2018, p.2). Moreover, according to Bennett and Livingston (2018, pp.134-135), the so-called 'disinformation order' results from more than the proliferation of 'fake news' is a mix of democratic institutional decline, public sphere disruptions and growing attacks on journalism and enlightenment values. Therefore, in order to address these new challenges one must have in mind the need to have a broader view, to assess the interplay between these disruptive processes in order to resist the easy efforts to make the problem go away by fact-checking initiatives and educating citizens about the perils of fake news. Furthermore, is also important to consider the changing dynamics in communication and the growing power and influence of global digital platforms. Big data analytics and algorithmic governance have increasingly become a new form of governance in societies, opening up new spaces of knowledge and control that did not previously exist, the implications of which are only now becoming evident. While bots, trolls and political advertisements may be short-term problems solvable by digital platforms in cooperation with governments globally, a far more fundamental challenge is the changing power dynamics between the two. Important decisions concerning sharing of information and content increasingly are being made by global corporations rather than societies. An absence of transparency and lack of access to the data provided by the digital platforms constrains researchers seeking to study the implications of this shift (Schia and Gjesvik 2020, pp.3-4).

2.2. Online Disinformation as a threat

Online disinformation has been at the top of the political agendas of states and international organisations, namely for being identified as a threat to democracy. Nevertheless, the conceptualisation of security in relation to threats such as online disinformation remains confused, unarticulated and underexplored, with implications for the development of an appropriate and proportional response (Ördén 2019, pp.421,422).

Thus, the objective of this sub-chapter is to understand the framing of online disinformation as a threat, namely to democracies. Firstly, it aims to understand the reason underlying the vulnerability of democracies to this challenge, by presenting the discussions concerning the strategic use of online disinformation and the asymmetric democratic disadvantage. Secondly, it aims to understand how can one understand online disinformation as a threat, by introducing the discussions on hybrid-threats, cyber-threats and as a threat to democracy.

2.2.1. The strategic use of Online Disinformation: motivations, means and effects

In the international realm, state-sponsored online disinformation as a foreign policy tool more than winning the battle of narratives, seek to influence public opinion and sow discord, to destroy the credibility of establish institutions of the target, in order to weakening the unity and to undermine the adversary from within (Nye 2019, p.10; Nicolas 2018, p.41). Consequently, the use of online disinformation as a foreign policy instrument can result for instance in the weakening of the legitimate authority of the government or the political system of the target; in the degradation of the national political discourse of the target; in the alteration of the perceived costs associated with certain policies pursued by the target, contributing to the employment other measures favourable to the attacker (Lanoszka 2019, pp.227,232-233; Gerrits 2018, p.5).

As previously mentioned, the strategic use of online disinformation as a foreign policy tool has mostly been associated with regimes such as Russia (Paterson and Hanley 2020, p.442; Bennett and Livingston 2018, p.132). The use of disinformation in Russian[25] foreign policy is not a novelty, however, digital technology and social media created new opportunities for the innovative employment of old methods such as active measures[26] (Jensen, Valeriano and Maness 2019, p.229; Cordy 2017, p.8).

Active measures are tactics with origins in traditional soviet military thinking, namely associated with KGB (the principal secret services unit of the Soviet Union), employed to influence in the international realm covertly. These measures are conducted secretly to influence the decision–making process of the target, namely to hinder its ability to gather public support for the pursuit of its policies, in a favourable direction or at least not harmful to the realisation of the objectives of the Kremlin. Active measures rely on the production and dissemination of disinformation through various channels, however the technological evolution, namely the emergence of cyberspace-tools enabled an innovative way to employ these tactics (Kragh and Asberg 2017, pp.778-779). In this scenario, the Kremlin has been employing coordinated efforts, using a mix of cyber-tools, hackers, troll factories and bots to produce and spread disinformation campaigns, namely through social media, in order to undermine the domestic political process of its target and destroy the enemy from within (Paterson and Hanley 2020; Jensen, Valeriano and Maness 2019; Bennett and Livingston 2018; Gerrits 2018). Russian sponsored-cyber operations have combined cyber-espionage operations and hacking of email accounts, to collect documents and information used to produce disinformation, afterwards spread and amplified through troll factories and bots. The St. Petersburg troll factory - Internet Research Agency (IRA) - is one of multiple Russian troll centres, with connections to the Russian government, that train and pay trolls to produce and

[25] We recognise that Russia is not the only state actor strategically employing disinformation domestically and internationally, neither authoritarian regimes, as previously mentioned. However, this focus emerges considering our analysis on the approach of the EU and NATO, both identify Russia has a central source disinformation. Moreover, multiple authors identify Russia and its influence in the 2016 U.S presidential elections as a game change that renewed attention towards state-sponsored information warfare (Paterson and Hanley 2020, pp.439, 442; Bennett and Livingston 2018, p.132).

[26] For a detailed understanding of 'active measures' see, for example, Giles (2016).

spread disinformation campaigns and generate chaos through digital platforms. According to Bennett and Livingston (2018, pp.132-133), in 2013, IRA employed around 600 individuals and had an estimated annual budget of 10 million US. In this company, trolls were paid to maintain six Facebook accounts and post at least three publications per day. On Twitter, they were expected to have at least ten accounts and tweet at least fifty times daily on each account. In both platforms, trolls had specific targets and objectives namely the number of users they need to gain attention. An empirical example of this combination is the 'pizzagate' case. In this case, Russian intelligence agents hacked email accounts of members of the Democratic National Committee, including John Podesta, the chair campaign of Hilary Clinton, and then IRA through its trolls produced and amplified disinformation campaigns and conspiracy theories that pointed out the involvement of Hillary Clinton as a leader of a network of child prostitution, aiming at damaging the Clinton campaign and promoting the Trump campaign (Paterson and Hanley 2020, pp.443-445).

The strategic use of online disinformation as a foreign policy tool by Russia is part of a domestic and geostrategic strategy that seeks to protect its own autocratic regime and strengthen its international strategic position, by disclosing the shortfalls of democracy (Paterson and Hanley 2020, pp.443-445; Bennett and Livingston 2018, pp.132-133; Gerrits 2018, pp.7-9). Hence, on the one hand, at the domestic level, Russian political and military actors consider western information warfare as a key security threat in its national security strategy. Therefore, overt and covert information operations, namely through disinformation, towards foreign audiences are employed to neutralise the adversary from within, but also as a response and as a defensive measure (Kragh and Asberg 2017, p.778). On the other hand, at the international level, Russia seems to be focused on sow confusion and discord in its targets, through ambiguous signalling and amplifying disinformation, rather than direct convincing and converting (Jensen, Valeriano and Maness 2019, p.229). This strategic usage seeks to erode public trust in democratic institutions, to undermine the domestic political process and to influence the external relations of its targets. Consequently, the Kremlin is perceived as an attacker that tries to "influence politics in 'the West'" (Monsees 2018, p.4) by disrupting the process of free deliberation (Monsees 2020, p.6), as a response to the pressure of NATO expansion and West reaction to Russian annexation of Crimean and interference in Ukraine (Bennett and Livingston 2018, pp.132-133). Nevertheless, this influence campaign does not proceed homogenously, and it has been reported in multiple countries, in the United Kingdom, in Germany, in the Netherlands, in Norway, in Sweden and in the U.S. Moreover, these campaigns acquire multiple shapes, in Ukraine, in the Baltic States, and in Eastern Europe seeks destabilisation and political influence; confusion in Western Europe; and distraction in the United States (Pomerantsev and Weiss cited in Gerrits 2018, p.10). Furthermore, in several countries domestic forces that are sympathetic with Russia have contributed to the amplification of these campaigns (Gerrits 2018, p.11).

Notwithstanding, the effects of the strategically usage of online disinformation as a foreign policy tool are debatable. Whereas Paterson and Hanley (2020) argue that the digital age not only reinforced the use and changed permanently the way states conduct these operations, it is also having a highly destabilising effect. Gerrits (2018) and Lanoszka (2019) consider that the security implications and the strategic effects shouldn't be overstated. Despite the deterioration of the international system, it does not alter the defence and foreign policy alignments of the target and therefore the balance of power. Additionally, Jakobsen (2019) highlights that "there is no evidence suggesting that Russian interference in western elections has made a decisive difference to their outcomes" (pp.160-161).

According to Lanoszka (2019, pp.227,238), three main obstacles prevent the success of disinformation in international politics. First, international anarchy generates uncertainty and consequently any international signal is open to multiple interpretations, which may not favour the attacker's goals. Second, pre-existing prejudices of the elites and citizens of the target mean that the malicious actor shouldn't be too obvious on disseminating disinformation, because the target can recognize and devalue it. Third, the target is not an inanimate object and can adopt counter-measures that minimize the impact of disinformation campaigns. Moreover, according to Jensen, Valeriano and Maness (2019, pp.214,229), the use of these operations reflect Russia's declining power. On the one hand, in conflict scenarios, such as Georgia and Ukraine, the use of cyber operations did not result in decisive victories or the achievement of strategic objectives. On the other hand, also the effects of the influence campaign in the 2016 U.S. presidential elections are debatable[27]. Furthermore, other experts alert that efforts made by foreign actors are limited and efforts by domestic actors is more worrisome compared to foreign (Schia and Gjesvik 2020, p.2).

However, despite the difficulty to accurately assess the effects of the strategic use of online disinformation by Russia, Paterson and Hanley (2020) argue that the perception of interference can be just as damaging as actual interference. As previously mentioned, the proliferation of disinformation is highly linked to a legitimacy and confidence crisis, particularly of citizens in

[27] Whereas the study of Allcott and Gentzkow (2017) challenged the influence of fake news on voting behaviour and on election results, other studies demonstrated that the spread of disinformation fosters polarisation (Del Vicario et al. 2016).

democratic institutions. Therefore, the perception of foreign interference in domestic democratic processes, and thus disclosing the incapacity of democracies to tackle these challenges, has the potential to reinforce the distrust and degrade western democratic legitimacy. Consequently, contributing to the success of the motivations underlying the use of online disinformation as a foreign policy tool (p.443). This argument is reinforced by a survey of citizens implemented by the European Council on Foreign Relations (ECFR) in 2018 in all EU Member States which concluded that the top five perceived threats are cyber-attacks, state collapse or civil war in the EU's neighbourhood, external meddling in domestic politics, uncontrolled migration and the deterioration of the international institutional order. Additionally, the respondents expect that the security threat landscape will remain focused on these challenges with the inclusion of terrorist attacks (Chappell, Mawdsley and Galbreath 2019, pp.191-192).

Hence, despite the antiquity and debatable effects of the strategic usage of disinformation in international politics, its potential role in disclosing shortfalls of the democratic systems, and thus contributing to the fulfilment of the objective of the attacker, evidences new tendencies that should be considered. On the one hand, although the ancient use of disinformation in international politics, nowadays democracies have a more assertive position, in understanding and addressing online disinformation as a security threat through security measures. On the other hand, at the same time, they acknowledge the challenge to respond without compromising the realisation of democratic values and principles such as freedom of expression. Thereby, democracies can be considered an easy target and a fragile responder, which strategies can generate other insecurities and represent a shift in the posture of democracies in the international system.

2.2.2. Online Disinformation: the democratic asymmetric disadvantage

The strategic use of disinformation to achieve political objectives is nothing new. However, there is a growing tendency to employ this strategy, in conflict areas, during political tensions and key political events (Tsaruk and Korniiets 2020, p.73). The examples vary from the use of disinformation in conflict scenarios, such as in the frozen conflict between Ukraine and Russia, to destabilise, undermine cohesion, fuel chaos, and compromise military decisions and actions (Willemo 2019; Danyk, Maliarchuk and Briggs 2017; Zeitzoff 2017); the use of disinformation to influence the outcome of elections, as was the case in the 2016 U.S. presidential elections (la Cour 2020; Paterson and Hanley 2020; Bennett and Livingston 2018); to the use of disinformation during the COVID-19 pandemic, to divert attention and preclude debate on the origins of the pandemic (Kurlantzick 2020).

In this scenario, both domestic and foreigner actors have been using disinformation domestically and internationally, namely to undermine democratic institutional legitimacy and destabilise centre parties, governments and elections, in order to achieve political objectives (Bennett and Livingston 2018, p.122).

At the domestic level, disinformation has been used by political actors, for instance by political candidates to achieve electoral goals, but also by journalists and citizens to advance partisan interests (Tenove 2020, p.519). These actors seek to block and contradict traditional media and provide followers with emotionally charged narratives that confirm their beliefs, through the creation of alternative information systems. In this context, particularly concerning political actors, extremist right movements have gained more attention, nevertheless this does not mean that radical left movements do not engage in disinformation campaigns. But, radical left movements have been more limited, particularly considering that their mobilisations do not translate into comparative levels of electoral success (Bennett and Livingston 2018, pp.127,132). Yet, it is important to note that, at the domestic level, the operation of the strategic usage of disinformation and the content varies according to national realities (Bennett and Livingston 2018; Humprecht 2018).

At the international level, disinformation has been used namely to subvert the democratic political process, to incite the proliferation of violence, and to challenge the sovereignty and values of democratic states (Paterson and Hanley 2020, p.439). Foreign actors have strategically used disinformation to target the domestic affairs of other countries, mainly the domestic political process of its targets as a sophisticated form of information warfare (Lukito 2020, p.239; Bennett and Livingston 2018, p.132).

Therefore, disinformation has been used at the national and at the international level, by domestic and foreign actors. Nevertheless, despite the dominant narrative that claims that foreign actors have played a prominent role in the production and dissemination of disinformation, analyses have demonstrated that domestic actors have played a major role (Tenove 2020, p.519). However, for the purposes of this study we focus on the strategic use of disinformation by foreign actors at the international level as a foreign policy tool.

In international politics, the strategically usage of disinformation to manipulate perceptions or to subvert political discourse is not new, but the growing proliferation of digital technologies allowed a more innovative employment of disinformation as a foreign policy instrument (Paterson and Hanley 2020, p.440; Schia and Gjesvik 2020, pp.1-2). Hence, online disinformation has been perceived as an alternative and less costly effort, employed in global power struggles, to strategically increase international influence and power (la Cour 2020, p.705; Nye 2019, p.10; Nicolas 2018, p.41).

Online disinformation has been employed by multiple state and non-state actors in international politics[28]. On the one hand, non-state actors, namely terrorists and extremist groups have been exploring digital technologies to spread disinformation in order to fulfil strategic objectives, from recruitment purposes to the spread propaganda. On the other hand, the use of disinformation by states has mostly been associated with regimes such as Russia and China (Paterson and Hanley 2020, p.442; Bennett and Livingston 2018, p.132). Nevertheless, both authoritarian and democratic regimes have used digital technologies to employ innovative forms of information warfare, through disinformation, in order to achieve a relative position of advantage in the international realm (Jensen, Valeriano and Maness 2019, p.213).

However, democracies are in an asymmetric disadvantage (Paterson and Hanley 2020, p.442). On the one hand, whereas in authoritarian regimes traditional media is controlled and dissent closely monitored, making it difficult for foreign influence campaigns and disinformation to succeed. The free flow of information and ideas expected in a democracy means that these systems are more vulnerable to be attacked with disinformation. On the other hand, the ability to address these campaigns by democracies is challenged by the need to balance between the response without compromising the realisation of democratic principles and values such as the freedom of expression. In addition, for instance, a tactic that has been employed to increase the spread of disinformation is the purchase of political advertisements on social media and the staging of social mobilisations. The response to these tactics is particularly challenging for democracies, because the purchasing of political ads, organising mobilisations and dissemination political propaganda is legal. Hence, launching an investigation requires strong evidence. Moreover, while provocative, the strategically use of disinformation is designed to be non-kinetic and non-lethal, exploring the grey zone between war and peace and remaining below the threshold of conflict, challenging the development and implementation of proportionate strategies (Paterson and Hanley 2020, pp.440-444). Furthermore, international law does not clearly prohibit influence operations, neither provide clear guidelines on how states can respond to foreigner disinformation campaigns. Define this type of regulation is challenging. Particularly considering online disinformation, while cyber-attacks that affect critical information infrastructures may clearly harm state functions, attacks

[28] For the purposes of this research we focus on state-sponsored disinformation campaigns.

in the form of disinformation usually affect beliefs, emotions and the cognitive process of individuals, which are difficult to regulate considering the uncertainty and subjectivity underling evidence, causation and motivations (Tenove 2020, pp. 522-523). Moreover, the present disagreement at the international level on what represents responsible use of cyber operations, particularly what forms of espionage and political interference are acceptable, should remain (Cavelty and Wenger 2020, pp.23-24).

2.2.3. Online Disinformation as a threat: as a hybrid threat, a cyber-threat and a threat to democracy

2.3.3.1 Online Disinformation as part of the hybrid threat landscape

Today, the complexity and the multiple forms that the challenges and threats to security may take have contributed to the emergence of concepts such as 'hybrid threats', 'hybrid war' and 'hybrid warfare'. According to Hoffman (2007, p.5), warfare is and will be conducted through the combination of diverse instruments, by flexible and sophisticated actors, who consider that success in conflict situations depends on the diversified use of tools. Accordingly, nowadays classifying a conflict as conventional or irregular is over simplistic, considering that state and non-state actors will tend to combine conventional and non-conventional instruments. Thus, according to Hoffman (2007, p.7), today and future warfare will be marked by the blurring lines between war and peace, therefore being hybrid, meaning that it will

> "...incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder...can be conducted by both states and a variety of non-state actors. These multi-modal activities...are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of conflict..." (Hoffman 2007, p.8).

Therefore, hybrid warfare can be conducted by state and non-state actors who use, in an integrated and coordinated way, in the same operations theatre, multiple conventional and non-conventional tools, in order to obtain synergic effects in the physical as wells as in the psychological dimension of the conflict.

However, despite the attention on hybrid threats and hybrid warfare and its primacy in the political agendas of states and international organisations, the debate on the association of hybrid to war has been contested and many academics and analysts criticise the analytical and empirical utility of the concept. This is the case mostly because there is an exaggeration on the novelty of the concept, which can be misleading and it does not capture the new elements; its imprecision and elasticity is more confusing than enlightening; moreover, its association with 'warfare' can be potentially dangerous by unnecessarily militarize the language of international politics (Wigell 2021, p.49; Wigell 2019, pp.255-256; Cormac and Aldrich 2018, p.477).

Hybrid threats and hybrid warfare have been labelled often as a new form of warfare and have been applied often to explain Russia's assertive behaviour. Thus, various academics use the concept of 'hybrid warfare' to describe the external action of the Kremlin in Eastern Ukraine and the success in annexation of Crimea as a result of the implementation of hybrid tactics. Furthermore, the understanding of this form of warfare as new challenges the utility of the use of force, considering that there is a growing perception on the preference to use non-conventional and non-military means such as disinformation. Accordingly, there is a perception that a new form of warfare is emerging that will be dominated by the psychological dimension and by information warfare in order to surpass the military dimension of warfare through the moral and phycological destabilization, reducing the need to use force (Berzins 2014). However, the coordinated use of military and non-military instruments its not new neither exclusive Russian (Popescu 2015). Moreover, the perception that Russia is focused on the non-conventional and non-military dimension of warfare is narrow and can be misleading as far as it concerns the analysis and understanding of the external action of Russia and defence strategies and policies (Giles 2016; Renz 2016). Furthermore, the novelty of hybrid threats does not lie in the tactics, but in the political, military, technological and social context in which they are employed that has changed, allowing a more efficient and easier use of hybrid tactics (Wigell 2019; Galeotti 2016).

On the other hand, activities that occur in the spectrum between war and peace may vary significantly, target different dimensions and have different degrees of intensity and effect. Thus, labelling non-military tactics similarly to military tactics may trigger potentially dangerous and disproportionate process of securitization. Accordingly, practices that are based on military means should be differentiated from those relying on non-military means considering that they require different counter-measures (Wigell 2019, p.256). Consequently, according to Wigell (2019), the lack of distinction between military and non-military contributes to treat Russia intervention in Eastern Ukraine and Crimea and the meddling in the 2016 US Presidential elections as belonging to the same threat categories, despite the former have involved the use of force (p.259).

Wigell (2019) proposes an alternative understanding by introducing the concept of hybrid interference, as "a 'wedge strategy', namely a policy of dividing a target country or coalition, thereby weakening its counterbalancing potential…draws on a panoply of state-controlled, non-kinetic means that are concealed in order to provide the divider with official deniability and manipulate targeted actors without elevating their threat perceptions" (p.256). The means that are employed in hybrid interference are clandestine diplomacy, geoeconomics and disinformation (Wigell 2019, p.256).

Therefore, the understanding of online disinformation as a security threat has been often associated to the framework of hybrid threats, as being part of the hybrid threat landscape, namely as the sophisticated and successful element of these type of threats.

2.3.3.2 Online Disinformation as part of the cyber-threat landscape

Despite the attention that emerging cyberspace-related challenges and threats have been gaining on the political agendas of states and international organisations, the understanding of cyberspace[29] as a security problem[30] is recent (Barrinha and Carrapiço 2016; Cavelty 2016). The evolution and proliferation of information and communication technologies into all aspects of contemporary societies – political, military, economic, and social – created new strategic possibilities, from social interaction, delivery of services to governance. However, this digital

[29] The term cyberspace has its origins in two fiction stories from William Gibson on the influences of cyberspace on human species, "Burning Chrome" (1982) and "Neuromancer" (1984), and was later on imported into the political realm by John Perry Barlow, a cyber-libertarian and activist (Barrinha and Carrapiço 2016, p.246; Cavelty 2013, p.107). This research understands cyberspace beyond electronic and computer related activities. Cyberspace is a domain made of electromagnetic activity and interconnected networks that allow electromagnetic activity to carry information, and electronic technology. Hence, by enabling the transmission of information, cyberspace has been used and considered an operational domain. As such, individuals and organisations use cyberspace to create, store, modify, exchange and exploit information in order to act and create effects in or across other domains (Robinson, Jones and Janicke 2015, pp.71-72). It is also important to note that cyberspace is virtual and physical. Virtual, considering the electromagnetic activity, and physical, because it involves servers, cables, satellites, computers and other physical devices that allow electromagnetic activity. Thus, "is the fusion of all communication networks, databases, and sources of information into a vast, tangled, and diverse blanket of electronic interchange" (Cavelty 2016, p.401). For a detailed understanding of the concept of cyberspace see, for instance, Barrinha and Carrapiço (2016); Cavelty (2016); Robinson, Jones and Janicke (2015); Cavelty (2013); Kello (2013); Nye (2010).

[30] The conceptualisation of an issue as an issue of security can be explained through the lens of the notion of Securitization. Securitization refers to the process by which a securitizing actor articulates an already politicised issue as an existential threat to a referent object. Consequently, in response, extraordinary measures beyond the ordinary measures, means and norms of the political domain should be adopted (Emmers 2010, p.139). The concept of securitisation is further discussed in chapter one (sub-chapter on conceptual framework).

dependency has, simultaneously, made states and societies more vulnerable to criminal activity and other security threats in and across this domain. At the same time, the strategic context of the post-Cold War era, reinforced by the events of 9/11 - based on the notions of asymmetric vulnerabilities associated with the multiplication of new non-traditional actors willing and capable to compete in order to shape the digital domain according to their strategic interests - have influenced the development of policies concerning the security of cyberspace (Deibert 2017, p.172; Barrinha and Carrapiço 2016, p.248; Liaropoulos 2015, p.15; Cavelty 2010, p.181).

According to Cavelty (2010, p.181), the debate on cyber-threats and the need to implement countermeasures to address them at the political level was introduced in the late 1980s in the United States of America, gained greater momentum in the mid-1990s and it spread to other countries in the late 1990s.

Between the late 1970s and the early 1980s, the technological evolution, particularly the merging of telecommunications with computers meant that any individual with a computer and a modem could exploit and intrude computer networks. Consequently, multiple events, from politically motivated attacks, computer viruses to the penetration of networks for criminal purposes generated political attention for the use of cyberspace for malicious and hostile purposes, particularly in association with a traditional discourse on espionage. Events such as the hacking perpetrated by the Milwakee-based '414s'[31] in the early 1980s demonstrated willing and capability to intrude government and other high level computers. In this scenario, there was a perception that if a group of teenagers were able to easily penetrate government networks, more structured and organised entities such as states could be even better equipped to intrude and access confidential and sensitive information for espionage purposes. The Cuckoo's Egg incident in 1986-1988[32] reinforced this association between unauthorised external computer intrusions and espionage purposes. Notwithstanding, considering that these attacks mainly affected governmental networks, the need to protect cyberspace did not receive much attention from the wider society (Cavelty 2016, p.403; Cavelty 2010, pp.181-182).

The association of cyberspace to the political and security spectrum was reinforced in the context of the Gulf War (1990-1991). The Gulf War is often considered to be the first information war, as a result of the recognition of the relevance of the strategic use of information and communication technologies for military effectiveness. In this scenario, U.S. military

[31] For a detailed understanding of this cyber-incident see, for instance, Cavelty (2016).

[32] An international KGB effort, that was only discovered by chance, to connect to computers in the U.S. and copy information from them (Cavelty 2016, p.406).

strategists acknowledged that the isolated use of military force was insufficient and there was a need to also dispute the information war and secure information dominance. Consequently, numerous academic publications in the U.S. emerged, emphasizing the advantage of degrading or even paralysing and opponent's communication systems (Cavelty 2016, p.408; Cavelty 2010, pp.182-183). According to Cavelty (2010, 2016), the context underlying NATO's 1999 intervention in Yugoslavia – Operation Allied Force – was the first time that the full-spectrum of information war components were used in combat. In this context, it involved the use of propaganda and disinformation through traditional media, extensive distributed denial-of-service attacks on several websites, and some rumours of alleged attacks to Yugoslavian leader Slobodan Milosevic's bank accounts by the US armed forces. Furthermore, the intense use of the internet by all sides involved in the conflict, including actors not directly involved, for the publication and sharing of conflict-relevant information meant that it was also the first war that used cyberspace to combat (Cavelty 2016, p. 410; Cavelty 2010, p.183).

However, in the mid-1990s, the advantages of the use of information and communication technologies were accompanied by the perception that the growing dependency on these technologies is also associated with a great vulnerability. The widespread use of these technologies by the military and the society in general meant that the use of information components was a double-edge sword. Consequently, through cyberspace an attack does not demand costly, specialised weapons, systems or armies and the non-existence of borders means that cyberspace become an alternative to launch an asymmetric attack against a civilian or a military critical infrastructure. In this scenario, activities of information warfare that were limited to the military and contexts of crisis or war began to be employed to the entire information structure of the adversary through a continuum of operations from war to peace (Cavelty 2016, p. 408).

Until the early 1990s the concepts of cyberspace and security evolved separately. Initially, the term 'cyber-security' was associated with technical problems and was used by computer scientists to refer to insecurities related to networked computers and to the need to protect data existing in computer systems as well as the computer systems themselves against unauthorised external intrusion (Barrinha and Carrapiço 2016, p.248; Hansen and Nissenbaum 2009, pp.1155-1160).

However, in the mid-1990s, the growing proliferation of information and communication technologies to multiple sectors of society contributed to the need to take action on the security of cyberspace and cyber-threats catapulted into the political agendas of states. The widespread use of digital technology meant that the referent object of security concerned the totality of critical information infrastructures that provide the way of life that characterises today's societies (Cavelty 2016, p.403; Cavelty 2010, pp.181-182).

Key sectors of contemporary states and societies, including those vital to national security and to the essential functioning of industrialised economies, depend on multiple highly interdependent national and international software-based control systems for their smooth, reliable and continuous operation. Consequently, governments, the private sector and civil society have come to consider the centrality of cyberspace and the potential for the political and social effects of malicious and hostile use of computer systems and their implications for security, resulting in the securitisation of cyberspace (Deibert 2017, p.172; Cavelty 2010, p.182; Hansen and Nissenbaum 2009, p.1155). This securitisation[33] entails two interlinked core elements, one technical and one social. On the one hand, the technical element is related to the network character of computer systems, meaning that these systems control physical objects such as trains, pipelines, and electrical transformers. In the event of a cyber-attack, these systems can be compromised, which in turn can hinder or prevent electrical or communication distribution, disrupt transportation systems, disable financial transactions, and consequently generate chaos (Hansen and Nissenbaum 2009, p.1161). On the other hand, there has been a transference or a duplication of human activity to the digital domain, at the personal and at the public and commercial level. At the personal level, a panoply of electronic devices is connected to cyberspace, such as personal computers, cell phones and home appliances. Therefore, the common citizen communicates, learn, socialise, work, buy and does almost everything through a permanent and omnipresent connection with cyberspace. At the public and commercial level, there has been a growing tendency towards the search for public (e-government) and commercial services online. Therefore, a growing number of essential daily processes – political, economic and social – have come to rely on the digital domain, which is based on open networks designed to be efficient and that don't have security as priority. Consequently, this scenario has been accompanied by a growing perception of cyberspace as a vulnerable domain to criminal activities as well as other types of threats to security (Barrinha and Carrapiço 2016, pp.247-248; van der Meer 2015, p.195; Cavelty 2010, p.182). This perception has solidified in recent years, considering that there is an impression among political actors that cyber-incidents[34] are becoming more frequent, more organised and sophisticated, more costly,

[33] For a detailed understanding of this securitisation process see, for instance, Hansen and Nissenbaum (2009, pp.1155-1175).

[34] Cavelty and Wenger (2020) understand cyber-incidents as "disruptions of the routine operations of digital technologies" (p.5).

and more dangerous. Consequently, measures to promote a safer cyberspace and cyber-security have come to hold a prominent position in national and international security policy. Accordingly, cyberspace-related insecurities and threats expanded beyond a technical issue to be also considered as a security issue and a top priority of global politics in the 21st century. This transformation of cyberspace into an object of security – securitisation of cyberspace – has influence the development of cyber-security (Cavelty and Wenger 2020, p.5; Deibert 2017, pp.172-173; Balzacq and Cavelty 2016, p.1; Barrinha and Carrapiço 2016, pp.246-248).

Despite its prominence in national and international security politics and widespread usage, at the governmental and at the academic level, the concept of cyber-security is recent and remains a contested and contestable concept[35] (Barrinha and Carrapiço 2016, p.248). This results from the technological infrastructure per se, designed for efficiency and not for security purposes; by the multiple problems underlying the lack of conceptual clarity that change across time and political contexts; and by the difficulty to coordinate the various aspects associated with the security of cyberspace (Balzacq and Cavelty 2016, p.5; Barrinha and Carrapiço 2016, pp.248,253, 259; Liaropoulos 2015, pp.16-17). Consequently, the formulation and implementation of cyber-security policies and strategies have focused on the needs of the state, ignoring or in some cases even contradicting the needs of its citizens, with implications for the comprehensive construction of a safer cyberspace.

Since its inception, that computer networks and the internet are inherently insecure. The internet, as a dynamic evolution of the ARPANET (Advanced Research Projects Agency Network), was designed to optimise the exchange of information. The emphasis was on the robustness and survivability of the network and, because it involved very few computers there was no apparent need for a specific focus on security. This understanding accompanies modern systems, that use the same network technology, in association with a shift to smaller and more open systems, and with the rise of extensive networking. Consequently, today's networks are more interconnected and more open, but security remains neglected, because is expensive, there is no direct return on investment, and security mechanisms have a negative impact on usability, hence security is often scarified for functionality (Cavelty 2016, p.401).

The absence of a clear definition of cyber-security also challenges the development and effectiveness of policies and strategies to secure the cyberspace. This situation partially results

[35] Moreover, the understanding of the concept of cyber-security differs not only at the governmental, but also at the academic level. The security of cyberspace has been analysed through the lenses of multiple disciplines, which have different classifications, methodologies, taxonomies and categorizations (Tsaruk and Korniiets 2020, pp.64-65).

from the lack of a universal accepted definition of cyberspace, there is no clear consensus on "what needs to be protected?" and on "need protection from what?". Consequently, there are plethora of terms related with the security of the cyberspace - information security, information and communication technologies security, network security, internet security, critical information infrastructures protection. Therefore, cyber-incidents are linked to different, but often inter-related, threat categories, that consider specific threat representations and referent objects; with different political, economic and social effects; and in need of different and sometimes conflicting responses – cyber-crime, cyber-terrorism and cyber-war[36] (Cavelty and Wenger 2020, p.7; Balzacq and Cavelty 2016, p.5; Barrinha and Carrapiço 2016, pp.248,253,259; Liaropoulos 2015, p.16).

Moreover, the understanding of cyber-security changes over time, mainly due to technological evolution and its implications, and it also changes according to the political context (Cavelty and Wenger 2020, p.7; Deibert 2017, pp.175-176).

On the one hand, initially, cyber-security was a technical risk management issue and computer scientists were mainly concerned with the insecurities and disruptions related to networked computers and the need to protect those networks from unauthorised external intrusion and different types malwares (Cavelty 2016, p.403). Nowadays, beyond being a technical risk, cyberspace is considered a domain of operations and cyber-incidents are a top priority on the political agendas of states and international organisations. The widespread digitalisation of contemporary states and societies, and the use of cyberspace to assert power and achieve domestic and foreign-policy interests by state and non-state actors, resulted into the understanding of cyber-security as a key national and international security issue (Cavelty and Wenger 2020, p.7; Deibert 2017, p.173; Cavelty 2010, p.184).

On the other hand, governments do not understand neither address cyber-security homogenously, mainly because states have different political agendas, interests, priorities, and capabilities. Therefore, there is a variation in terms of what is consider to be the scope and nature of threats – which can include crime, espionage, anonymous hacktivists, content deemed offensive or illegal, online activities of radical and extremist militant groups, manipulation of information, and organised anti-regime mobilisation – and the referent object of cyber-security (Deibert 2017, pp.175-176). In this scenario, for instance, according to Tsaruk and Korniiets (2020, pp.58-60), the United States and international organisations such as NATO and the EU

[36] For a detailed understanding of these three concepts see, for instance, Deibert (2017), Barrinha and Carrapiço (2016), Cavelty (2016) and Cavelty (2010).

understand and address cyber-security and information security differently from countries such as Russia and China. The USA/NATO/EU understand information security as part of cyber-security, and in the majority of western liberal societies there is a restraint to implement information security strategies, considering the potential for contradiction between the realisation of basic human rights and the management of information flows. Whereas countries as China and Russia understand cyber-security as part of information security and place more emphasis on the later, which is generally equated with regime security (Tsaruk and Korniiets 2020, pp.58-60; Deibert 2017, p.175). Nevertheless, rigid delimitations should be made carefully, as there are numerous examples where similarities are as striking as the differences, and many grey areas where rhetoric and practice do not align, as the Edward Snowden revelations demonstrated (Deibert 2017, p.175).

Consequently, governments have been representing threats in and through cyberspace differently, with implications for the political response (Cavelty, 2013) – from cyber catastrophists, digital realists to techno-optimists (Lacy and Prince 2018).

Cyber catastrophists have a pessimistic perspective about cyberspace and claim that the digital disaster is a reality and a central threat in the future. In this scenario, catastrophists speculate about the occurrence of a cyber-war, a cyber 9/11 or even a cyber Pearl Harbour, in which communication systems may collapse, transport networks may paralyse and the money of thousands of people may be inaccessible, generating widespread chaos (Lacy and Prince 2018, p.104; Eriksson and Giacomello, 2006, p.226). This perspective asserts that cyber-security should be understood and addressed as a national security issue (Liaropoulos 2015, pp.15-16; Cavelty 2013, pp.118-119).

However, despite this understanding is to a certain extent justified it is also deficient and entails two problems. On the one hand, in this scenario, cyber-security policies and strategies have been developed and implemented not based on actual harm, but on the disruptive potential of cyber-threats. Accordingly, a picture of a potential 'cyber-doom' and the anticipation of future disasters, rather than past experiences or solid justifications of current level of threat, inform cyber-security policies and strategies (Barrinha and Carrapiço 2016, p.245; Cavelty 2016, p.414; Cavelty 2010, pp.180, 184). This catastrophic understanding has been unsubstantiated, considering that none of the worst-case scenarios have so far materialised and cyber-incidents have been mostly a business and espionage problem, rather than a national security issue (Cavelty 2016, p.415; Cavelty 2010, p.187). Therefore, the effects of cyber-incidents have been so far very limited (particularly in terms of human lives and physical resources) and debatable, namely considering that evidence on cyber-incidents is often anecdotal, particular considering the uncertainty underlying the identity, actual capabilities and intentions of potential adversaries (Barrinha and Carrapiço 2016, p.245; Cavelty 2010, p.184). On the other hand, embracing a catastrophic cyber-war perspective bears the danger of creating an atmosphere of tension and insecurity, generating a cyber-security dilemma, establishing a situation of mutual distrust that has the potential, and has resulted in a cyber-arms race (Cavelty 2016, pp.410, 415; Kello 2013, pp.32-33).

Digital realists have a more optimistic perspective about cyberspace and are critical of the hypersecuritization[37] underling the prospect of a cyber-war (Lacy and Prince 2018, p.106). Accordingly, despite the challenge posed by the malicious and hostile use of cyberspace its implications should not be overstated. Cyber-war never happened, it is not happening and it will unlikely happen in the future. According to Rid (2012), what has been experienced in cyberspace are sophisticated forms of sabotage, espionage and subversion[38]. Nevertheless, this does not mean that the danger of cyber-threats should not be taken into consideration, but that there is a need to build informed and appropriate cyber-security policies, in order to avoid high-costs with uncertain or low benefits, and prevent the development of detrimental countermeasures that have the potential to create new insecurities (Cavelty 2016, p.415; Cavelty 2010, pp.184, 187).

Techno-optimists have an optimistic perspective about cyberspace and on technological evolution more broadly. Optimists admit the occurrence of cyber-incidents, however the capability to address these vulnerabilities will be progressively improved through research, scientific knowledge and education (Lacy and Prince 2018, pp.109-110). Accordingly, this representation of cyberspace is accompanied by an organic response, linked to the aspiration for self-healing, self-organisation and decentralisation (Cavelty 2013, pp.118-119). Consequently, the role of the state should be limited to that of facilitator, and the main concern of this perspective stems from the fear of these digital technologies being used by states for surveillance purposes. Therefore, the main goal should be to prevent the "militarization or 'Balkanization' of the internet" (Lacy and Prince 2018, p.110; Cavelty 2013, pp.118-119).

In this scenario, Liaropoulos (2015) argue that there is a tendency to address cyber-security in a negative way. Accordingly, on the one hand, based on a negative perspective, security is understood as the absence of threats to core human values. On the other hand, in a positive

[37] Hypersecuritization refers to the expansion of a security issue to a domain where there is the danger of exaggerating threats and develop and implement excessive counter-measures. For a detailed understanding of this concept see, for instance, Hansen and Nissenbaum (2009).

[38] For a detailed understanding of these concepts see, for instance, Omand (2018) and Rid (2012).

perspective, addressing security means safeguarding and empowering individuals to freely and securely exercise their rights (p.19). In cyber-security there is a tendency to pursue a negative approach, by addressing mainly the needs of the state, ignoring or in some cases even contradicting the needs of its citizens (Deibert 2017, p.173). According to Deibert (2017, p.173), cyber-security has been used as a surveillance instrument, justified by an 'anti-terror' or 'cyber-crime' discourse and laws, that critics worry it has the potential to contradict the realisation of human rights and civil liberties. Events such as Edward Snowden's revelations about the global surveillance carried out by the U.S. National Security Agency challenge Internet freedom, anonymity and data protection. Consequently, citizens can be the cyber victims of national security policies and not its beneficiaries. Moreover, there is an increasing tendency to block content on the internet. The rational and the content to be filtered varies from country to country. From the need to control access to content that violates copyright, illegal content associated with child exploitation or that promotes hatred and violence, to the filtration of content associated with minority rights, religious movements, political opposition and human rights groups. These measures are not exclusive of non-democratic systems. Furthermore, digital platforms have also been used as intermediaries to detect, isolate and contain organisers and participants of social mobilisations (Deibert 2017, pp.173,176-178).

Gio, Goodman and Wanless (2019, p.117) argue that this situation can be explained by the narrow conceptualisation of cyber-security by governments, practitioners and academia that tends focus mostly on the physical and logical domain of cyberspace, ignoring is social dimension. Traditional conceptualisations of cyberspace include the physical, the logical and the social layer. In this scenario, according to Gioe, Goodman and Wanless (2019), cyber-security means that "if these three layers are secure, the system or network itself must be secure" (p.117). However, despite the social layer being the most vulnerable one, its security has been marginalised comparing to the other two layers. Conceptual difficulties related to the social layer has in general justified the lack of attention to this layer. Furthermore, in practice, is easier to secure computers and systems, by installing patching software to protect against identified flaws and avoid unauthorized external intrusion; than to patch citizenry and protect societies from social engineering, propaganda, disinformation and extremist or terrorist recruitment circulating across digital platforms, namely on social media. Therefore, the physical and the logical layer have been at the top of the agenda, not only because of conceptual challenges related to defining security at the human and societal interface, but also because it is easier to secure a network than secure societal cohesiveness and cognitive resilience (Gioe, Goodman and Wanless 2019, p.117). Notwithstanding, the attack vectors available in cyberspace have been expanding, spying and DDoS attacks (distributed denial of service attacks) are now accompanied by influencing the public opinion on domestic affairs (Tsaruk and Korniiets 2020, p.57). In a time of unprecedented volumes of online disinformation there is an urgent need to re-think traditional notions of critical infrastructure and to rebalance between the three layers of cyberspace, namely a greater commitment towards the comprehension and security of the social layer. Hence, there is a need to cope with more traditional and obvious cyber-incidents, such as shutting down connectivity or compromising email. But, at the same time, it should be considered subtler ones such as subverting activities through the spread of disinformation on social media. The development and implementation of cyber-security policies and strategies should consider beyond the protection of critical information infrastructures and address cyber-security through a human-centric perspective that considers digital human rights, violations, Internet freedom and privacy of data. That "patch the social layer vulnerabilities" and beyond the engagement of coders, network administrators and programmers, also non-tech people, from social sciences for instance, must be involve to make cyberspace secure (Gio, Goodman and Wanless 2019, pp.117-118; Zittrain 2017, p.300; Liaropoulos 2015, p.18).

2.3.3.3 Online Disinformation as a threat to democracy

Although the debate on the effects of international online disinformation is inconclusive and controversial (Humprecht, Esser and Aelst 2020, p.494; Bjola 2017, p.189), governments, academics and citizens have expressed preoccupation that its strategic employment may threaten democracy and should be considered and addressed as a security threat. Consequently, governments and international organisations have been formulating and implementing multiple policies and strategies from the security sector, from offensive cyber-operations targeting actors that spread disinformation to regulation of social media platforms (Tenove 2020, p.517).

Notwithstanding, the analysis on what it means for online disinformation to threaten democracy and how different policies and strategies might protect democracy is in need of clarification. Especially because, according to Tenove (2020, p.519), the response to online disinformation has been politicised. Therefore, policy decisions and responses to address or not online disinformation have the potential to advantage or disadvantage specific political actors. Hence, on the one hand, the response to online disinformation may be accompanied by democratic risks. The formulation and implementation of strategies to address online disinformation may be instrumentalised to attack journalists or political opponents. Moreover, addressing online disinformation has become emotionally charged. Thus, policy responses have the potential to be formulated as a response to humiliation caused by false stories or by anger that arises from knowing that foreign actors have influenced domestic affairs (la Cour 2020, p.709; Tenove 2020, p.519). On the other hand, the absence of a response to online disinformation may constitute an attempt to empower specific actors. Ignoring the need to address online disinformation may be an effort from the incumbent governments to block reforms or preclude debate, justified by concern that addressing online disinformation threatens the realisation of fundamental rights such as the freedom of expression (Tenove 2020, p.531).

To what extent online disinformation is considered to be a threat and part of a broader contemporary security landscape, to which democracies are particularly vulnerable, remains unclear. This study identifies three perspectives in the academic debate on how online disinformation can be understood and framed as a threat to democracy and particularly as a security threat: online disinformation has been considered a threat to democracy considering its relation to three main themes (Monsees 2020); online disinformation as threat to three normative goods underlying the democratic system (Tenove 2020); and online disinformation as an existential threat to the future of human civilization (Lin 2019).

On the one hand, whereas Monsees (2020) presents a broader analysis of disinformation as a threat to democracy, as a result of its relation with three main themes: ‘hate speech and the use of social media’, ‘disinformation and democratic deliberation’, and ‘Russia as a geopolitical threat’ (p.6). Lin (2019) goes even further to consider disinformation as a threat to the future of human civilization based on the pillars of logic, truth and reality. On the other hand, Tenove (2020) proposes a narrower approach, by understanding disinformation as a threat to three normative goods underlying the democratic system, particularly to accountable representation and to the deliberation process, but mostly to the self-determination of citizens to enact freely and fairly in democratic life.

Firstly, according to Monsees (2020, p.6), the understanding of disinformation as a threat to democracy results from its linkage to increasing levels of populism, racist and xenophobic tendencies, and hate speech, particularly spread through social media. These tendencies have the potential to cause disruption in societies, justifying its inclusion in the threat framework. In Germany, for example, disinformation did not have much impact on parliamentary elections of 2017. Nevertheless, the continuous spread of false stories about refugees is perceived as major concern in a context marked by an ongoing debate on refuges and the rise of right-wing populism.

Secondly, online disinformation has been understood as a threat to democracy because it threatens the deliberation process (Monsees 2020; Tenove 2020; Lin 2019).

Tenove (2020, pp.518,531) identifies three normative goods of democracies that are claimed by governments to be threaten by disinformation: self-determination, accountable representation, and public deliberation promoting opinion and will formation. Despite its interconnections, each represents a different aspect of the democratic system that can be harmed by disinformation, demanding different policy responses. Therefore, the threat to self-determination is mainly addressed by security policies at the national and international level. These policies are design to respond to threats to key state activities, such as the enforcement of election laws and to ensure that full and fair participation in the democratic processes is not undermined by actors with malicious or hostile intentions. The threat to accountable representation is addressed by new electoral regulations, design to protect fundamental rights of the citizens, such as the right to vote and prevent efforts that compromise fair and transparent electoral processes. The threat to public deliberation is addressed by media regulation, design to protect freedom of expression and to cultivate media systems capable of producing a robust and morally respectful communication. The objective of this study is to analyse how online disinformation is understood and addressed as a security threat, thus we focus our attention on the threat pose by online disinformation to self-determination.

The understanding of disinformation as a threat to self-determination results from the association of the strategic use of this type of information with its potential to undermine the ability of citizens to enact in democratic life, "if it compromises the selective empowerments that enable citizens to…(vote in fair elections, or to freely contribute to public discourse on political issues)", and ultimately as a threat to the sovereignty of states. In this context, disinformation has been perceived as a threat to the foundational process of democracy – the process of a rational and democratic deliberation (Tenove 2020, p.522). The supporting infrastructure of a healthy public sphere[39] is under tension and thus the democratic process itself. News and truth have a central role in democratic societies, considering their role in rational debate and in the formation of an informed public opinion, which is a key factor of the democratic process. The existence and sharing of disinformation contributes to permanent exposition of citizens to falsehoods and manipulated information, which in turn can generate

[39] Nevertheless, it is important to note that disinformation in general and online disinformation in particular are symptoms of the chaos on the contemporary public communication framework and are not the only reason behind what Wardle and Derakhsan (2018) termed as 'information disorder'. There are other challenges in the journalistic industry: the financial decline of traditional media, which in turn means less staff available to fact check and with tighter and more competitive deadlines; the digital transformation, with opportunities and challenges for the creation, distribution, circulation and consume of news. For a detailed understanding of these dynamics see, for example, Morgan (2018) and Posetti (2018).

persistent misperceptions, polluting the democratic process on its source (Monsees 2020, pp.7-8; Paterson and Hanley 2020, pp.440,442; Egelhofer and Lecheler 2019, p.102; Morgan 2018, pp.39-40; Roozenbeek and van der Linden 2018, pp.1-2; Tandoc Jr., Lim and Ling 2018, pp.137-138; Bjola 2017, p.189; McGonagle 2017, p.204). Consequently, has claimed by Lin (2019, pp.188-189), disinformation can be understood an existential threat to the future of human civilization. Accordingly, the infrastructure that supports human civilization is under threat. This infrastructure is tangible, it is physical, chemical and biological, but it is also increasingly virtual, considering the information ecosystem, critical to the realisation of multiple activities of contemporary states and societies. Hence, the prosperity and advancement of contemporary societies is highly linked to the security of the information infrastructure and environment, which supports the thinking and decisions of individuals with contextualised, reliable, trustworthy information.

Thirdly, the threat of disinformation has also been understood as part of broader discussions on hybrid warfare, cyber-security and information warfare (Monsees 2020).

In this context, understanding disinformation as a security threat has been discursively linked to the representation of Russia as the major source of disinformation. Accordingly, there is a perception that Russia has been strategically employing disinformation campaigns to target the democratic process of its targets, namely the deliberation and electoral process, as part of a geopolitical strategy. Consequently, the strategic use of disinformation is understood as a military threat. Concerns underlying the democratic process merge with national security concerns, thus the threat of disinformation to the deliberation process becomes an existential threat to national security (Monsees 2020, pp.8-9).

Furthermore, according to Lukito (2020, p.239), state-sponsored disinformation campaigns targeting foreign audiences can be considered as an interference into the internal affairs of another country and can be violation of Westphalian sovereignty principles. Nevertheless, traditional understandings on intervention and the requisite of coercion codified in international law do not currently encompass the use of social media and digital disinformation (Nicolas 2018, p.53). Moreover, some theorists argue that foreigners should have a role in influencing the domestic process of other states considering the present globalised world, the actions of one state can have repercussions on other states. However, this situation should be limited and not be deceiving means (Tenove 2020, p. 522).

Despite its debatable effects, online disinformation has been framed and addressed as a threat to democracy and as part of a broader contemporary security framework through multiple discourses. According to Tenove (2020 p.524), addressing disinformation as a security threat is often appropriate, considering its potential to undermine the ability of governments and citizens to enact in democratic life. Moreover, security agencies, through for instance intelligence, are better prepare to collect information about the source and support a more effective response. Nevertheless, on the one hand, these security organisms have complicated relation with democracy, because they tend to be under weak democratic control and can contribute to excessive influence in the democratic process by the incumbent government or by security agencies themselves. On the other hand, the use of security laws against disinformation in authoritarian countries is well-documented, but there are also emerging concerns that some democracies have been employing policies that can contradict democratic principles such as the freedom of expression.

The securitisation of disinformation holds democratic risks and has the potential to expose democracies shortfalls, consequently contributing to the success of the motivations underlying these campaigns. Accordingly, it is essential to understand how disinformation has been framed and addressed as a security threat, in order to support the formulation of appropriate and proportionate solutions to tackle this phenomenon. Therefore, the next chapters analyse the discursive construction in security terms and the security governance of online disinformation at EU level to evaluate by means of case study the preoccupation with this dilemma underlying the response to disinformation in democratic societies.

CHAPTER 3

The discursive construction of Online Disinformation in security terms: The Case of the European Union

The objective of this chapter is to analyse the discursive construction of online disinformation in security terms by the European Union, aiming to understand how the EU normatively justifies its moral ground to respond against this type of content. Accordingly, it answers the following questions: *How does the European Union discursively constructs online disinformation in security terms? How the European Union normatively justifies the need to respond to online disinformation?*

The preoccupation with the phenomenon of disinformation at the EU level is not new and has been mostly associated with the distance between the Union and its citizens. The political and the institutional complexity underlying the European Union has contributed to the relative distance between the Union and its citizens, which has been exploited by politicians to misinform and deceive on issues concerning the EU (Hedling 2021).

The European Union recognises this lack of proximity with its citizens since, at least, 2001. In 2001, within the scope of the White Paper on European Governance the, at the time, Commission of the European Communities acknowledged the increasing distance and distrust of European citizens in politics and in political institutions more broadly and in the European Union in particular. This distance was perceived as resulting from the distrust and the poor understanding of the EU as well as of the complex system underlying European politics. Accordingly, European citizens do not understand the European project and tend to perceive the EU as a remote entity that suffers from democratic deficit, associated with the complexity underlying the decision-making processes and mechanisms; with the absence of a parliamentary chamber to hold governmental accountability; with the failure of political elites to involve citizens on the direction and objectives of the integration process; and reinforced by the image often portrayed by the media and national political leaders of the EU as a source of unpopular political decisions (Cini and Borrogán 2013, p.7). Moreover, this sentiment has been accompanied by a paradoxical perception of the EU by European citizens that simultaneous see the European Union as a remote entity and too intrusive. Consequently, since at least 2001 that, within the framework underlying the reform of the European governance, the EU aims to improve the connection between Europe and the European integration project and its citizens (Commission of the European Communities 2001).

Accordingly, the European Union has been struggling to communicate with European citizens, particularly with regard to the explanation underlying the rational for integration and in generating some sense of identification with the European project, with implications for the spread of disinformation in the context of the EU (Hedling 2021; Cini and Borrogán 2013, p.7).

However, despite the concern with the relative distance between the European Union and its citizens and its potential to be exploited as a channel to misinform and deceive, only in 2015 has disinformation been officially recognised as a challenge in need of response and only since 2016 has it gained a prominent position in the political agenda of the Union and in security-focused initiatives (Carrapiço and Farrand 2020, p.1118).

In 2015, the need to "challenge Russia's ongoing disinformation campaigns" (European Council 2015) in the eastern neighbourhood prompted the EU's discourse and policy response to disinformation. Disinformation was perceived as an external threat with origins in Russia to the strategic objectives of the Union in the eastern neighbourhood. Hence, initially, the rational underlying the response to disinformation was related to the realisation of the foreign policy objectives of the European Union in the eastern neighbourhood. Ergo, the security logic to address disinformation was guided by an external perspective, illustrated by the invitation from the European Council to the High Representative to suggest an Action Plan on Strategic Communication to address this challenge and by the creation of a Strategic Communication Team in the European External Action Service.

Nevertheless, since 2016, the changing security landscape, the constant use of hybrid threats and cyber-threats in the form of disinformation and the various election processes occurring in Europe and in particular the 2019 European Parliament elections represented a turning point for the EU in terms of the rational underlying the discursive construction of disinformation as a threat. The dissemination of disinformation campaigns as a vehicle for hybrid threats was considered as a mean to exploit the vulnerabilities and to manipulate the decision-making process of the European Union (European Commission and High Representative 2016). Hence, beyond the rational of framing disinformation as a challenge to the realisation of the foreign policy objectives of the Union, disinformation came to be recognised as a "major challenge for Europe", as threat to the European security and to the survival of the European integration process itself (European Commission 2018a). Consequently, introducing the internal dimension underlying the challenge of disinformation, particularly illustrated by the inclusion of the European Commission in the response equation in addition to the role of the High Representative and of the European External Action Service.

Moreover, disinformation has come to be understood by the European Union not only as a threat to its internal security and domestic democratic processes, but also that this threat may also have its source inside the EU itself. Ever since, disinformation has been discursively constructed as a threat to European democracy, to the realisation of human rights and fundamental freedoms, but also as a threat to the realisation of the Digital Single Market and the European Digital Sovereignty and more recently with the COVID-19 pandemic crisis as a threat to public health.

At the same time, the European Union has been recognising that disinformation may take multiple forms and uses different tools with consequent different security logics of response. Accordingly, the European Union uses the term disinformation to refer to different phenomena, disinformation includes disinformation in the narrow sense, misinformation, information influence operations and foreign interference in the information space (European Commission 2021b). Therefore, *Disinformation* is understood as "false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm". Public harm comprises threats to the democratic political and policy-making process, as well as to public goods such as the protection of EU citizens health, the environment or security. *Misinformation* is understood as "false or misleading content shared without harmful intent though the effects can still be harmful, e.g. when people share false information with friends and family in good faith". *Information influence operations* is understood as "coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including supressing independent information sources in combination with disinformation". *Foreign interference in the information space* "often carried out as part of a broader hybrid operation, can be understood as coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents" (European Commission 2020a).

Consequently, considering the multiple phenomena associated with disinformation, the European Union recognises the need to take into account the differences between them in order to calibrate appropriate responses, demonstrating from the inception of the response to disinformation a preoccupation with a proportional response. First, it is important to consider the distinction between illegal and harmful content, while disinformation content is usually harmful it is not illegal. Second, it is important to determine whether there is an intention to deceive and cause public harm or, if the dissemination of these campaigns aims for economic gain. Therefore, on the one hand, whereas disinformation in the form of misinformation has the potential to be harmful, its non-intentional nature means that the response should be calibrated and based on the improvement of resilience through the identification, analysis and exposure of disinformation campaigns as well as on media literacy initiatives. On the other hand, interference and influence operations by foreign countries usually combine different actions, including disinformation, such coordination suggests a strategic intention to cause harm. Thus, demanding a more assertive and coordinated response that involves actions taken by governments, digital platforms, particularly social media (European Commission and High Representative 2020c).

Therefore, the discursive construction of online disinformation in security terms by the European Union is not straightforward and this study identifies four main rationales that have been guiding this discursive construction: a strategic and security rational, a political rational, an economic rational, and more recently a public health rational. Despite these different rationales it is important to note that it does not mean that they occur separately, they influence and have implications for each other. The analysis of these different rationales aims to determine the normative justification underlying the response of the European Union to online disinformation.

3.1. Strategic and Security rationales: Disinformation as a threat to the foreign policy objectives of the EU and as a hybrid threat

In the European Union, Russia’s ongoing use of disinformation in the Eastern Neighbourhood prompted a more assertive discourse and the development of policies and strategies to tackle this challenge (Giumelli, Cusumano and Besana 2018, p.152; Bjola and Pamment 2016). Initially, the rationale underlying the response of the EU towards disinformation was mostly strategic, linked to the realisation of the foreign policy objectives of the Union in the Eastern Neighbourhood, translated into the invitation from the European Council to the High Representative to suggest an Action Plan on Strategic Communication and by the creation of a Strategic Communication team in the European External Action Service. The changes in the security environment, namely the growing emergence of the use of hybrid threats mostly by Russia, particularly in the form of disinformation, were accompanied by a security rationale associated with the external-internal security nexus. This is illustrated by the Joint Communication from the European Commission and the High Representative on countering hybrid threats: a European Union response that acknowledges the need to adapt and increase the capacities of the European Union as a security provider considering the intimate relationship between external and internal security. Accordingly, the multiple challenges to internal peace, security and prosperity have its origins in the instability in the EU's immediate neighbourhood (European Commission and High Representative 2016). This assumption is reinforced by the Action Plan against Disinformation that recognises that exposing disinformation in neighbourhood countries, in the Eastern and Southern Neighbourhood as well as in the Western Balkans is complementary to tackling the problem within the Union (European Commission and High Representative 2018a). Therefore, initially, the discursive construction of disinformation as a threat at EU level is based on strategic and security rationales. The strategic rationale assumes that disinformation is a threat to the external action of the Union in the Eastern Neighbourhood and the security rational assumes that hybrid threats in the form of disinformation is a threat to the strategic objectives of the EU in the eastern vicinity, but is also a threat for the EU itself. Consequently, the need of response emerges because these understandings of disinformation as a threat has implications for the EU's external action and security, but also for its role as a credible and a reliable actor and partner in the area of security and defence.

In January 2015, a two-page informal paper presented by four EU Member States (Denmark, Estonia, Lithuania, and the United Kingdom[40]) identified the need to set up an action plan at the EU level to counter Russian propaganda. The use of disinformation campaigns by Russia was considered a security threat at the eastern borders of the EU, because of their impact on discrediting EU narratives; challenging the support for legitimate governments in the region; demoralising local populations; and confusing western policymakers (Euobserver 2015). Hence, the concern with the using of communication tools by Russia, particularly in the form of disinformation, was related to their effects in the political, economic and security context in the Eastern Neighbourhood and consequently to the realisation of the objectives of the Union in the region.

Accordingly, in the European Council of 19th-20th of March 2015 it was acknowledged for the first time at the EU level the need to "challenge Russia's ongoing disinformation campaigns", prompting the policy action of inviting the High Representative to present an Action Plan on Strategic Communications in June 2015 and the creation of a Strategic Communication Team in the European External Action Service (European Council 2015).

[40] The United Kingdom is no longer an EU Member State since 31st of January 2020.

Thus, the association between the threat of disinformation and Russia's action in the Eastern Neighbourhood, particularly in Ukraine, is reinforced by the 2015 European Council, that frames the need to address the challenge of disinformation in the section concerning External Relations in the point on Russia/Ukraine. Furthermore, at the same time, this preoccupation was accompanied by the revision of the European Neighbourhood Policy (ENP), the Eastern Partnership Summit in Riga and the condemnation of the annexation of Crimea and Sevastopol and subsequent sanctions and the implementation of Minsk agreements. The Eastern Partnership Summit that took place in Riga[41] between the 21st and 22nd of May with the purpose of reinforcing the commitment of the EU towards the Eastern Neighbourhood namely in relation to the deepened cooperation in state building, mobility and people-to-to people contacts, market opportunities and interconnections, was accompanied by multiple events that demonstrated the preoccupation with public communication. In this context, the First Eastern Partnership Media Conference aimed at analysing the challenges underlying traditional media and pluralism in the Eastern Partnership countries and improving the media context in the region. Moreover, the Second Eastern Partnership Civil Society Conference focused on strengthening the role of civil society in partner countries.

Therefore, in order to better understand the initial strategic rational of the discursive construction of disinformation as a threat it is important to consider the dynamics underlying the interaction of the EU in the Eastern Neighbourhood and with Russia.

Casier (2012) argues that this interaction should be analysed within the framework of a triangle that considers the three main players – the European Union, Russia and the neighbouring state, because all three relationships have the potential to mutually influence each other. The cases of Georgia and Ukraine illustrate the potential effects of domestic dynamics on the relations of these countries *vis-à-vis* the EU and Russia, but also on EU-Russia relations[42]. Despite the constraints related particularly to economic dependence, the neighbouring country is an important player that influence the success of the policies of the EU and Russia in the common neighbourhood (pp.33,46,49). The focus of this study is on the interaction between the EU and Ukraine and between the EU and Russia, because, as previously

[41] This Summit was attended by on the one hand the EU, represented by the President of the European Commission, the President of the European Council, the High Representative of the Union for Foreign Affairs and Security Policy, the President of the European Parliament, the Commissioner for Neighbourhood Policy and Enlargement Negotiations, the Commissioner for Trade, and Member States. On the other hand, by Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine.

[42] To better understand these dynamics, see, for instance, Delcour (2018); Nitoiu (2016); Haukkala (2015); Matsaberidze (2015); Dias (2013); Averre (2009).

demonstrated, the preoccupation with disinformation is identified in the section on Russia/Ukraine.

First, it is important to consider the interaction between the European Union and the neighbouring state, in this case Ukraine, understood within the context of the European Neighbourhood Policy. The European Neighbourhood Policy emerged following the enlargement of the EU to former satellite states of the Soviet Union and the Baltic states[43]. On the one hand, the neighbouring states saw in the European Union a way to support their political and economic transitions, and return to Europe. On the other hand, through enlargement and the prospect of membership the EU aimed to stimulate political and economic reforms in the potential candidates, aiming at promoting stability in the entire region (Cini and Borragán 2013, pp.4-5). The enlargement implied a new geopolitical position of the EU, translated into the extension of the organisation further East and into the subsequent creation of new frontiers. This situation produced concerns about the proximity to the instability on the EU's Eastern borders and the potential emergence of new dividing lines. Consequently, in 2004, in order to overcome these preoccupations, the European Neighbourhood Policy was created and implemented with the purpose of developing privileged relations with the new neighbourhoods (Casier 2012; Fernandes 2012).

The starting point of the European Neighbourhood Policy can be traced to the European Council that took place in Copenhagen in December 2002. In this European Council the enlargement of the European Union was considered an opportunity to deepen the relations between the EU and its neighbours, mostly because the increasing porosity of the frontiers was accompanied by the understanding that an event occurring outside the Union have the potential to impact the EU itself (Commission of the European Communities 2003, pp.3-4). Moreover, in 2003, in the framework of the European Security Strategy, the EU reinforces this assumption by acknowledging the relevance of the stability in the neighbourhood for the security of the EU (Council of the European Union 2003, pp.16-19). Accordingly, the increasing porosity of traditional frontiers was translated into the dissolution between internal and external security, meaning that the security of the European Union starts beyond its borders. This idea is demonstrated in the Communication of the European Commission to the Council and the European Parliament "Wider Europe — Neighbourhood: A New Framework for Relations with our Eastern and Southern Neighbours", "Over the coming decade and beyond, the Union's

[43] Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia accessed in 2004, Bulgaria and Romania joined in 2007 and Croatia in 2013.

capacity to provide security, stability and sustainable development to its citizens will no longer be distinguishable from its interest in close cooperation with the neighbours" (Commission of the European Communities 2003, p.3).

In 2004, following the enlargement of the European Union to ten new member states from Central and Eastern Europe[44], the European Neighbourhood Policy was created with the purpose of overcoming two important strategic issues post-enlargement. On the one hand, the policy aimed to avoid the creation of new dividing lines between an enlarged Europe and a fragile neighbourhood, and the edification of a 'European fortress' that would convert the European Union into a closed region for development and stability (Fernandes 2012, p.83). On the other hand, the ENP was produced in order to promote stability, security and prosperity in the Union and for its neighbours without the prospect of membership (Korosteleva 2011, pp.1-2). Consequently, according to Casier (2012) "through this policy the EU gave itself a higher degree of responsibility in Eastern Europe" (p.34).

Therefore, the ENP can be understood as an alternative to the enlargement policy, that aimed to promote stability, security and prosperity in the vicinity of the Union in order to manage the challenges associated with the internal-external security nexus, but without the prospect of membership. Hence, the European Union considers the neighbourhood simultaneously as an opportunity and as a challenge. On the one hand, Christou (2010) argues that the action of the European Union in its neighbourhood results from the preoccupation with the fragile governance in these states and its potential to create political instability and economic crises; with the growing transnational criminal activity; and with the multiple ongoing armed conflicts in the region with potential implications for the stability and security of the European space. On the other hand, the EU sees in the neighbourhood an opportunity to promote and spread its peace project based on its history of integration, through which by regional cooperation prevented the emergence of new armed conflicts (Delcour 2010, p.538). Hence, in order to protect the European peace project, the EU aims to project its normative model based on democratic values, the rule of law and the protection and promotion of human rights in its vicinity. Moreover, it projects an image of proximity, cooperation, friendship and shared goals in order to prevent the creation of new dividing lines (Christou 2010, pp.415-416)[45].

[44] Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovenia and Slovakia.

[45] For better understanding of the discussions on the European Neighborhood Policy see, for instance, Cadier (2019); Nitoiu and Sus (2019); Freire and Simão (2013); Korosteleva (2011).

This policy involves the European Union and sixteen neighbourhood countries in the Eastern Neighbourhood, North Africa and Middle East[46] and is implemented through bilateral action plans agreed between the EU and each partner country. These action plans are designed with the focus on the political and economic reform of each partner country. The ENP was reinforced by the Eastern Partnership (EaP). This initiative was introduced by Poland and Sweden at the beginning of 2008 on the May 26 Council of the European Union, approved by the European Council in June, operationalised in a Communication from the European Commission on December 3 and officially launched in May 2009 at the Prague Eastern Partnership Summit. This partnership was created to strengthen the objectives of the ENP, particularly the promotion of stability and prosperity at the Eastern borders of the EU, and to provide a better offer to the Eastern neighbourhood partners without offering membership guarantees. According to Fernandes (2012), the EaP highlighted multiple shortcomings of the ENP and the need to address more consistently the issue of transition in Armenia, Azerbaijan, Georgia, Moldova, Ukraine and Belarus, which were considered to constitute a problematic *de facto* in the common neighbourhood between the EU and Russia (p.84).

In this scenario, Fernandes (2012) relates the deepening of the eastern dimension of the external action of the EU and the development of a situation of tension in Europe, particularly with Russia (pp.84-85). Hence, the enlargement strategy and the inception of the Eastern Neighbourhood Policy and Eastern Partnership were accompanied by a widespread assumption that the European Union and Russia have been competing for influence in the region of the common neighbourhood (*ibid* p.31). Nevertheless, Casier (2012) argues that the dominant assumption on the competition between the EU and Russia is not sufficient to analyse their interactions. However, their relation has been mostly based on rivalry and for the purposes of this study this dimension is highlighted, particularly considering the situation of increasing tension between Russia and the West in 2022 with Ukraine once again as a stage of rivalry[47]. Therefore, the realisation of the objectives underlying the external action of the European Union

[46] Algeria, Armenia, Azerbaijan, Belarus, Egypt, Georgia, Israel, Jordan, Lebanon, Libya, Moldova, Morocco, Palestine, Syria, Tunisia and Ukraine.

[47] On the 24th February, 2022 President Vladimir Putin, in its official discourse, authorised the launching of a ‘special military operation’ and invaded Ukraine with the intention of demilitarisation and denazification, following an alleged sentiment of threat. The ongoing war in Ukraine amplified the implications concerning the use of disinformation particularly in the context of wartime, reinforcing its threat character. Disinformation has been used in this context and has been met at the European Union level with a new more assertive type of response – blocking – which will be further discussed in the next chapter.

in the Eastern Neighbourhood through the ENP and the EaP should consider the relation between the EU and Russia.

The relation between the European Union and Russia is debatable at its foundation, because both parts have different understandings with regard to the meaning of partnership. Jakobsen (2019) argues that "in the western perspective, partnership was about westernising Russia" (p.155). Accordingly, the partnership is based on the transformation of Russia according to EU standards of liberal western democracy and open market economy. Whereas, in the Russian perspective, the partnership does not exist because the West, particularly the EU and NATO through the implementation of enlargement policies, continually disrespect the great power interests and aspirations of Russia specially in the "near abroad" (*ibid* p.156). Russia remains deeply connected to its imperial past, illustrated by Vladimir Putin perception on the collapse of the Soviet Union as the biggest geopolitical disaster of the century and by its consideration of the former Soviet states as a sphere "it wished to maintain a high degree of influence" (Casier 2012, pp.34-35).

Accordingly, the relation between the West and Russia has been featured at the minimum by divergence, with implications for the progress of the relationship, but, as previously mentioned, also for the realisation of the objectives with other players in the common neighbourhood. On the one hand, the enlargement of both NATO and the EU, the creation of the European Neighbourhood Policy and the Eastern Partnership were perceived by Russia as an attempt from the West to deepen its influence in the common neighbourhood and consequently as threatening, this sentiment has been reinforced as demonstrated in the context of the events of February 2022[48]. In respect to the external action of the European Union in particular, the implementation of the ENP and the EaP were met with the launching of the Eurasian Customs Union (ECU) by Russia. The position of the EU concerning the incompatibility between the ECU membership and the Association Agreements of the EaP, the intention of the 2014 Ukrainian government to deepen the integration with the EU through the signing of the Association Agreement were accompanied by hybrid warfare tactics, the annexation of Crimea and the proxy warfare in Eastern Ukraine by Russia. This security tension was reinforced with the events initiated in February 2022[49]. Nevertheless, Russia rejects accusations of being waging hybrid warfare and accuses the West of employing hybrid warfare long before 2014, in Serbia (2000), Georgia (2003), Ukraine (2004-2005) and Kyrgyzstan

[48] See note 45.

[49] See note 45.

(2005), and justifies its actions as a form of protection of Russian minorities. However, despite the evidence that suggests the involvement of the West in the above-mentioned revolutions its impact was limited (Jakobsen 2019). On the other hand, the European Union and NATO deny these accusations and perceive them mostly as a form to legitimise the use of force by Russia in Ukraine. Furthermore, both organisations highlight the use of hybrid warfare tactics by Russia against the West, involving the persistent and coordinated use of instruments and tools such as disinformation campaigns, cyber-attacks against critical infrastructures and private sector (Jakobsen 2019, pp.156-157,159). There is increasingly little doubt that Russia has been actively trying to destabilise the West through a campaign of hybrid threats, particularly in the form of disinformation campaigns (Chappell, Mawdsley and Galbreath 2019, p.192).

Consequently, disinformation has been at the top of the political and security agendas of western governments and international organisations. In the case of the European Union, this evolution in the security environment has been met with the acknowledgment of disinformation by Russia not only as a challenge to the realisation of the foreign policy objectives in the eastern neighbourhood, but also as a threat to the EU itself particularly in the form of hybrid threats.

This is preoccupation with disinformation in security terms is demonstrated in the European Union's Foreign and Security Policy of 2016, where the EU recognises that threats as hybrid threats endanger the security of the Union and there is a need to enhance efforts to, among multiple areas on strategic communications, namely on improving the consistency and spread of messaging on principles and actions.

The EU recognises that information warfare and the use of disinformation as integral part of hybrid warfare are not new (European Parliament 2016). In this context, disinformation campaigns disseminated with origins in Russia are of particular concern at EU level. The Action Plan against Disinformation notes that the EU Hybrid Fusion Cell identifies Russia has the greatest threat to the EU in terms of disinformation, mostly because it is systematic and well-resourced (European Commission and High Representative 2018a). The March 2018 Salisbury chemical attack[50] and the related European Council conclusions contributed to an enforcement of the action towards hybrid threats. Consequently, resulting in the Communication of the European Commission and High Representative on bolstering resilience against hybrid threats, in which disinformation was again identified as a vehicle for hybrid threats and strategic

[50] The Salisbury attack refers to the poisoning of Sergei and Yulia Skripal. Sergei Skripal is a former Russian military officer and double agent for the British intelligence agencies, who along is daughter Yulia Skripal were poisoned on 4th of March 2018 in Salisbury, England. According to official sources in the United Kingdom and the Organisations for the Prohibition of chemical Weapons the poison was provoked by novichok nerve agent and linked to Russia.

communication was identified as a priority field. Hence, reinforcing the strategic rational and preoccupation of the use of this type of strategy as part of a broader coordinated effort to interfere in the information space of EU region, in order to threaten the EU Member States' sovereignty, political independence, the security of its citizens and its territorial integrity. This understanding is reinforced in the context of the events of February 2022, demonstrated by the EU's position to adopt exceptional measures, particularly through the blocking strategy translated into the suspending some Russian channels from broadcasting in the Union, which will be further discussed in chapter six[51].

At the same time, the European Union reinforces the assumption underlying the internal-external security nexus in respect to hybrid threats in the form of disinformation by recognising that the use of disinformation campaigns in the territory of partner countries should be perceived as an early sign. Accordingly, in the 11th December 2017 Council of the European Union on strengthening of European Union-Ukraine cooperation on internal security, the EU "recognises hybrid threats [including disinformation] which Ukraine has been confronted with, as an early warning sign to the Member States about possible emerging internal security threats and views it as a possibility to learn from the experience of Ukraine" (Council of the European Union 2017).

In this scenario, at the EU level, the European Parliament recalls that security and intelligence services conclude that Russia has the intention and the capacity to conduct subversive campaigns through hybrid threats in the form of disinformation, but also by supporting national political extremists (European Parliament 2016). The EU identifies multiple instruments and tools through which Russia disseminates disinformation, such as think thanks and special foundations (e.g. Russkiy Mir), special authorities (e.g. Rossotrudnichestvo), multilingual TV stations (e.g. RT), news agencies and multimedia services (e.g. Sputnik), cross-border social and religious groups, social media and internet trolls, the funding of political parties and other organisations within the EU and the use of contacts and official meetings with EU counterparts. The use of disinformation by Russia is perceived by the EU as a strategy that aims to distort truth, sow doubt, gather domestic support and challenge democratic values, in order to discredit EU institutions and transatlantic partnerships before EU citizens and citizens of neighbouring countries, to influence the domestic decision-making process and created the

[51] For a broader and deeper understanding about the sanctions and the restrictive measures applied by the European Union against Russia over Ukraine since 2014 see, for instance, https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/.

perception of failed states in the EU's Eastern Neighbourhood, to weaken the sovereignty, political independence and territorial integrity of the Union and its Member States, to weaken EU cooperation and divide Europe, and to foment a strategic split between the EU and its North American partners (European Parliament 2016).

Therefore, on the one hand, the EU recognises the impact of the use of hybrid warfare tactics by Russia, particularly in the form of disinformation campaigns, in the objectives of the EU in the eastern neighbourhood. This is in part because there is a strong presence of Russian media in those countries that aims to confront the influence of the European Union and the national media is incapable of response. On the other hand, at the same time, the European Union notes that Russia has been disseminating disinformation campaigns in the EU space, with the purpose of gathering political support for Russian action in European public opinion and undermining coherence of the EU foreign policy. Consequently, these activities not only have the potential to impact the domestic politics and democratic decision-making process, but it is also recognised their potential to increase polarisation at the international level, hindering effective multilateralism and undermining international security and stability (European Commission and High Representative 2020a).

Moreover, it is important to note the element of coordination associated with disinformation as a vehicle for hybrid threats promoted by Russia. The EU recognises that despite the flexibility underlying the concept of hybrid threats it captures the combination of methods such as disinformation with cyberattacks, making disinformation more resilient (European Commission and High Representative 2016). This is demonstrated in the EU's Cybersecurity Strategy for the Digital Decade, "cyberspace is increasingly exploited for political and ideological purposes…hybrid threats combine disinformation campaigns with cyberattacks on infrastructure, economic processes and democratic institutions, with the potential for causing physical damage, obtaining unlawful access to personal data…sowing mistrust and weakening social cohesion" (European Commission and High Representative 2020a). Therefore, disinformation as part of hybrid threat campaigns is of particular concern, because it assumes a coordination of means that aims intentionally to do harm and to exploit "the vulnerabilities of the target and on generating ambiguity to hinder decision-making process" (European Commission and High Representative 2016).

Accordingly, the discursive construction of disinformation as a form of hybrid threat with origins in Russia is of particular concern, because it is associated with coordinated "coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will" (European Commission 2020a).

Furthermore, the strategic and the security rational underlying the discursive construction of disinformation in security terms is also related to the implementation of the security and defence agenda of the European Union more broadly. The conclusions on security and defence of the 10th May 2021 Council of the European Union and the European Council conclusions of 28th June 2018 identified the need to improve resilience of security and defence at the EU level, which should encompass, beyond traditional issues, countering hybrid threats, cyber-attacks and disinformation. The increasing of resilience and capabilities to respond to these threats are part of a broader objective that aims to cultivate greater responsibility for the security of the Union, but also to support its role as a credible and reliable actor in the area of security and defence. This is of particular importance because as Chappell, Mawdsley and Galbreath (2019b) noticed "Europe's security problems came at a time when the liberal world order that emerged after the cold war is being challenged" (p.199). The multiple crises that have unleashed in Europe – the sovereign debt crisis, the refugee crisis and so on – and the debatable capability of the EU to manage it have been accompanied by the resurgent of nationalism, by the action of domestic and foreign actors that have been promoting campaigns that aim to undermine democratic values and process, which contributed for instance to Brexit (Chappell, Mawdsley and Galbreath 2019, p.10; 2019, p.199).

Consequently, the European Union recognises the need to take more responsibility for its own security, and for that end, the response to threats such as disinformation has implications for the realisation of the EU actorness in the area of security and defence more broadly. This is reinforced in the Strategic Compass for security and defence 2022, created to make Europe a security provider. In this context the European Union reinforces its understanding of disinformation in security terms, "our world is becoming less free with human rights, human security and democratic values under attack – both at home and abroad. We face a competition of governance systems accompanied by a real battle of narratives" (European Union 2022). At the same time, this discursive construction is particular linked to disinformation produced by Russia in the context of its invasion of Ukraine and accompanied by a more assertive posture of the European Union in terms of the response to disinformation, as we will further discuss in chapter six. In this context, responding to disinformation is about protecting European citizens, values and interests as well as international peace and security, and this is particularly demonstrated by the intention of the European Union to also counter disinformation operations in the context of its Common Security and Defence Policy (CSDP) missions and operations (European Union 2022a).

To sum up, initially, the European Union discursively constructed disinformation as a strategic threat particularly in the context of its foreign policy objectives in the Eastern Neighbourhood and, as the security context evolved, as a security threat in the form of foreign interference in the information space. Accordingly, disinformation as a strategic threat is associated with the threat of the manipulation of the media framework by Russia to the realisation of the objectives of the Union in the shared neighbourhood. Moreover, disinformation as a security threat is understood as part of a broader hybrid operation that aims to disrupt the free formation and expression of individuals' political will. Therefore, the prospect of threat to democracy particularly in the context of electoral period has seen the major development and implementation of initiatives so far. Hence, the next sub-chapter analyses the discursive construction of disinformation as a threat to democracy and to the realisation of fundamental rights and freedoms.

3.2. Strategic and Political rationales: Disinformation as a threat to democracy and to the realisation of fundamental rights and freedoms

In the European Union, disinformation has been constructed as a threat to the foreign policy objectives in the Eastern Neighbourhood, as a hybrid threat, but also as a threat to democracy and to the realisation of fundamental rights and freedoms.

The discursive construction of disinformation as a threat to democracy results mostly from the concern with the potential increasing of targeted disinformation campaigns against the European Union, its institutions and policies during the 2019 European Parliament elections and also against more than 50 presidential, national and local elections that took place in Member States in 2020, demanding the need to secure free and fair democratic processes. The Communication of the European Commission on Securing Free and Fair elections highlighted the contextual singularity underlying these electoral processes, that occur in parallel with an international environment where states that do not share the same interests and values of the EU are competing for power and using interference strategies such as disinformation (European Commission 2018b). Consequently, the increasing concern with hybrid threats, particularly in the form of disinformation, and its potential use against the multiple electoral process occurring in Europe contributed to the discursive construction of disinformation as "major threat for Europe" (European Commission 2018a). This is because "disinformation often targets European institutions and their representatives and aims at undermining the European project itself" (European Commission and High Representative 2018a). Consequently, emerged a sense of urgency to respond in a proportionated and sustained manner without undermining the promotion and protection of fundamental human rights and freedoms (European Council 2018). Thus, in the European Union, disinformation is discursively constructed as part of the hybrid threat and the cyber-threat framework and also as a threat to the EU order and values (Carrapiço and Farrand 2020, p.1120). Furthermore, in this context, disinformation is highlighted as an external and as an internal issue, with origin outside, but also within the Union (European Parliament 2016). Accordingly, in this context, disinformation can be understood as disinformation *per se*, but also in the framework of information influence operations that considers coordinated efforts to influence an audience either by domestic or foreign actors. In this context, disinformation has been discursively constructed as a strategic threat to democracy and fundamental human rights and for that reason a threat to the existence of the EU itself, thus this discursive construction is guided by a strategic and a political rational.

In terms of the discursive construction of disinformation as a threat to human rights and fundamental freedoms, it is important to consider the understanding of freedom of expression at the EU level. Freedom of expression is a core value of the European Union, demonstrated in the European Union Charter of Fundamental Rights and in the Constitutions of the Member States. The European Union understands that freedom of expression encompasses "respect for media freedom and pluralism, as well as the right of citizens to hold opinions and to receive and impart information and ideas 'without interference by public authorities and regardless of frontiers" (European Commission 2018a). European democratic societies depend on the ability of citizens to access a plurality of verifiable information to form their opinion on different political issues in order to have an informed participation in public debates and in electoral process (European Commission and High Representative 2018a). Therefore, in this context, disinformation is discursively constructed as a threat to the realisation of fundamental freedoms, namely freedom of expression, because it prevents the realisation of citizens to receive information without interference. Consequently, information influence operations, particularly in the form of disinformation, are an attack and a threat to the realisation of freedom of expression, because it challenges the freedom of citizens from being manipulated.

This is also, at the minimum, indirectly underlined in the European Agenda on Security (2015) and in the EU Security Union Strategy (2020). Accordingly, in the European Agenda on Security the EU stress the need to "ensure that people live in an area of freedom, security and justice in full compliance with European principles and values" (European Commission 2015). In the EU Security Union Strategy, the EU reinforces that "security is not only the basis for personal safety, it also protects fundamental rights and provides the foundation for confidence and dynamism in our economy, our society and our democracy" (European Commission 2020b). In this context, the EU acknowledges that internal security is not only about safety, but also about the protection of fundamental rights, including freedom of expression, which provides the basis for confidence in democracy. Therefore, tackling disinformation is a mean to protect and promote the realisation of human rights and fundamental freedoms and strengthening the civic and political space, considering its effects in preventing freedom from manipulation, and also a meant to promote security at the EU level (European Commission and High Representative 2020b).

Disinformation is also and mostly understood as a threat to democracy. The Communications from the European Commission on Securing Free and Fair Elections (2018b) and on European Democracy Action Plan (2020a) particularly demonstrate this discursive construction, by recognising politically motivated disinformation as a threat to European democracy, especially during electoral periods. This is because of its underlying objectives of discrediting and delegitimising elections, by affecting citizens trust in the democratic process and the integrity and fairness of the electoral process. The European Union assumes that a healthy and resilient democracy is based, among other things, on an active, informed and empowered civil society, not only at election time, but all the time (European Commission 2020a). Moreover, the EU underlines that democratic societies depend on meaningful participation of its citizens, which are able to form their own judgements and participate in an informed way in the public debate, fundamental to the deliberative democratic process. The deliberate, large-scale and systemic dissemination of disinformation challenges this assumption, by polluting the democratic process at is source. Consequently, threatening democracy, by sowing confusion and distrust in the democratic process and democratic institutions, the proliferation of disinformation prevents the formation of an informed opinion free from interference and undermines the participation of citizens in the democratic process. Moreover, it is also a vehicle to supports radical and extremist ideas and activities (European Commission 2020a; European Commission 2018a; European Commission and High Representative 2018a).

Democracy is a core value of the EU and is in the DNA of the European Union, illustrated for instance by being one of the requirements to integrate the European project. In order to join the European Union candidates must sign the *acquis communautaire* (EU treaties, legislation and norms), but also shared common values as democracy, human rights and principles of social justice. Hence, in 1993, the Copenhagen European Council defined the Copenhagen criteria, political and economic standards that countries have to meet in order to join the EU, they must have market economies, liberal democracies and they must be able to comply with the *acquis communautaire* (Cini and Borrogán 2013, pp.3-4). Therefore, the threat of disinformation to democracy is being discursively constructed as a matter of security, because the threat of disinformation to democracy is a threat to "who we are" (European Commission 2018b). This is further reinforced in the Communication from the European Commission on Securing Free and Fair Elections (2018b), "ensuring the resilience of the Union's democratic systems is part of the Security Union".

To sum up, the European Union discursively constructs disinformation as a threat to the EU mostly because it is a threat to fundamental rights and freedoms and to European democracy, which is considered to be the foundational principle of the European integration project. In this scenario, disinformation is considered to threaten the democratic process and societies because it challenges the assumption of freedom from interference and manipulation underlying the democratic process of formation of opinion. Consequently, affecting the informed participation of citizens in the democratic process, particularly in times of elections. The participation of citizens is fundamental to the democratic process, thus disinformation pollutes democracy at is source, with implications for the integrity and fairness in the electoral process and citizens trust in democracy, and ultimately to the survival of democracy and the European project itself. Moreover, it contributes to the distrust in democratic structures and processes and can contribute to other forms of harmful and illegal content such as hate speech and incite violence online and offline.

3.3. Strategic and Economic rationales: Disinformation as a threat to the realisation of Digital Europe and European Digital Sovereignty

In the European Union, disinformation has also been discursively constructed as a threat with economic implications namely to the realisation of Digital Europe and European Digital Sovereignty.

The June 2017 European Council acknowledges the ambitious digital vision for Europe, its society and economy and the need to implement a Digital Single Market strategy, that considers the underlying emerging global, technological, security and sustainability challenges (European Council 2017a). The European Council recognises the multiple opportunities of digitalisation for innovation, progress, prosperity, growth, jobs creation, competitiveness, and for creative and cultural diversity. Nevertheless, digitalisation is also accompanied by multiple challenges, among which is disinformation, that affects the political and the social dimensions, but also the economic (European Council 2017b).

The 22nd March 2019 European Council acknowledged that a strong economy is fundamental for the prosperity and competitiveness of Europe as well as for the realisation of its leading role on the international stage. The Communications from the European Commission on Shaping Europe's digital future and on the 2030 Digital Compass acknowledged the importance of the digital transition for the progress, prosperity and digital sovereignty of the European Union (European Commission 2021a and 2020c). This is reinforced in the 2nd October 2020 European Council, that notes that the digital transition is one of the fundamental pillars underlying the recovery process from the COVID-19 pandemic crisis. Hence, the digital transition is fundamental for a strong European economy and consequently for the prosperity and competitiveness of Europe and the realisation of its digital sovereignty. Moreover, this transition should be accompanied by the safeguard of the values and fundamental rights promoted at the EU level and by the security of the European space. At the same time, the Union recognises the importance of integrating and addressing current and emerging global, technological, security and sustainability challenges, with particular focus on the digital transition (European Council 2019). Therefore, considering the impact of disinformation in the realisation of democratic values, fundamental rights and security in the digital space, as previously demonstrated, it is also understood as a threat to the realisation of the Digital Single Market, with potential implications for the European Digital sovereignty and leadership role on a global scale. This triad between the economy, the digital transition and the need to tackle disinformation is further demonstrated in the 23rd June 2017 European Council, that recognises the need to take a holist approach to the digital space and implement a strategy that considers all its elements, markets, infrastructure, connectivity, but also societal and cultural aspects and it welcomes the review of the European Cybersecurity Strategy that considers disinformation in the spectrum of cyber-security challenges.

Tackling disinformation means protecting foreign policy objectives, protecting the security of the EU, protecting EU democracy and human rights, and also means protecting the European economy and its international image as a trend setter at a global scale in terms of digital transformation. Accordingly, "For Europe to truly influence the way in which digital solutions are developed and used on a global scale, it needs to be a strong, independent and purposeful digital player in its own right. In order to achieve this, a clear framework that promotes trustworthy, digitally enabled interactions across society, for people as well as for business, is need" (European Commission 2020c). The response to online disinformation is of utmost importance to create a trustworthy digital environment that enables the creation of a digital single market and supports the build-up of European digital sovereignty. Hence, the realisation of a Digital Europe and the actively participation of the EU in the Digital Decade should be based on a system of digitally skilled, capable and empowered citizens in how they act and interact online. Therefore, the European Union recognises the importance of developing technological capabilities that empowers citizens and business to take advantage of the digital transition in order to build a prosperous and competitive society (European Commission 2021a). This is reinforced in the conclusions of the Council of the European Union on the EU's cybersecurity strategy for the digital decade, that highlights the fundamental role of cybersecurity for the creation of a resilient, green and digital Europe. This strategy should be focused on the building of resilience, technological sovereignty and leadership. At the same time, it should be based on the protection the citizens, business and institutions of the EU from cyber incidents and threats, and should focus on the improvement of trust on the EU's ability to promote a secure and reliable cyberspace that is global, open, free, stable and based on human rights, fundamental freedoms, democracy and the rule of law (Council of the European Union 2021b).

3.4. Public health rational: Disinformation as a threat to public health

The COVID-19 pandemic crisis emerged as a new channel to amplify the challenges posed by online disinformation, particularly at the health, economic and social levels. The pandemic has been demanding the implementation of measures of physical distancing and isolation, that have been translated into a growing dependency on cyberspace to operationalise multiple activities, at the personal, social, professional, economic and educational levels. In this context, malicious and hostile actors have been using cyberspace and social media to exploit vulnerabilities that result from increasing technological dependency associated with confinement, as well as from fear, anxiety, non-stop searching of information, absence of consensual information among specialists and the need to find comfort in simple explanations. At the same time, this crisis has been accompanied by an explosion of the flux of information – true, fake, of bad quality and manipulated-, strengthened by digitalisation, to which the World Health Organization has named *infodemic*. In this scenario, is of particular concern the proliferation and dissemination of disinformation on social media, contributing to the discursive construction of disinformation as a threat to public health at the EU level.

Disinformation campaigns disseminated on social media associated with the pandemic crisis have been demonstrating the potential and multiple effects of these campaigns on-line and off-line. For instance, multiple messages spread across social media that question the existence of the virus and others that propose miracle cures with chloroquine or alcohol have already contributed to multiple situations of intoxication and poisoning. Moreover, conspiracy theories particularly about 5G, assuming that this infrastructure is a channel to spread coronavirus, have contributed to the destruction of more than 70 telecommunication poles and the persecution of several engineers in the United Kingdom (Spring 2020). Furthermore, the pandemic crisis has been capitalised by extremists' groups to amplify hate speech and hate crimes against multiple communities. A study conducted by BBC Click and the think-tank Institute of Strategic Dialogue have identified the following target-groups that have been accused of spreading the virus, migrants, Muslim community, Jewish community and LGBT Community. Additionally, also some elites have been targeted with conspiracy theories, for example George Soros and Bill Gates have been associated with the creation and the origins of the pandemic (Miller 2020).

At the same time, the scientific community is being pressure to provide scientific and factual information as soon as possible. However, the communication of science has been ineffective so far, mostly because there is a lack of explanation and understanding concerning the progress of scientific research and the production of knowledge, particularly in relation to the common initial disagreements – epistemic uncertainty associated with the initial phase – which increases the lack of trust in scientific knowledge. Consequently, it enables the resilience of online disinformation campaigns, and contributes to an increasing distrust in traditional actors which are usually sources of information – political actors, traditional media and scientific community. Therefore, there is a need for the scientific community to communicate effectively and transparently, in order to avoid the lack of trust of citizens and the potential appropriation of this empty space by movements such as the anti-vaccination (Roose 2020).

The European Union acknowledged the implications of online disinformation associated with the pandemic crisis, introducing the rational of understanding online disinformation as a threat also to public health. This is demonstrated in the Guidance on Strengthening the Code of Practice on Disinformation (2021b) from the European Commission that recognises that the sudden increasing dependency on cyberspace for every daily activity has the potential to increase the exposition of citizens to *infodemic* and particularly to disinformation, with implications for personal health, public health systems, crisis management and economic and social cohesion (European Commission 2021b). Moreover, the Security Union Strategy

(2020b) also highlighted that the divisions and uncertainties underlying the crisis also created a security vulnerability with implications for the potential increasing of more sophisticated hybrid attacks particularly in the form of disinformation (European Commission 2020b).

In addition, the European Union also highlighted the complexity and resilience of disinformation in the digital age particularly considering that it can take multiple forms and be used in combination with other forms of attack. Moreover, although disinformation *per se* is not criminal and illegal in nature, its use and combinations may be related to illegality and crime. This is acknowledged in the Joint Communication from the European Commission and the High Representative on Tackling COVID-19 disinformation – Getting the facts right (2020c) that identifies some examples. First, hoaxes and misleading healthcare information, such as 'it does not help to wash your hands' or 'the coronavirus is only a danger to the elderly', are not illegal *per se*, but can be harmful and undermine the efforts undertaken to respond and contain the pandemic. This type of content can deceive citizens to ignore official health and scientific information and engage in risky behaviour. Second, conspiracy theories may have implications and be associated with illegal and criminal actions, such as myths about the role of the 5G infrastructure in the spread of the virus have been accompanied by attacks on masts and engineers. Moreover, conspiracy theories about particular ethnic or religious groups being responsible for the origin and the spread of the virus have been feeding hate speech and have been associated with a worrying rise of related racist and xenophobic content. Third, another example is the use of deceiving information in consumer fraud, such as the selling of miracle products based on unsupported scientific information. Forth, the combination of misleading information with cyber activities of hacking and phishing that use COVID-19 related links to spread malware. Fifth, foreign actors and third countries, particularly Russia and China, have been targeting influence operations and disinformation campaigns about the spread and the response to COVID-19 in the EU, its neighbourhood and globally, aiming at undermining the democratic debate, amplifying social polarisation, undermining the image of the EU and its member states, particularly in relation to the response to the pandemic, in order to improve their own image (European Commission and the High Representative 2020c).

In conclusion, today, the European Union considers online disinformation in security terms, mostly because it threatens the survival of the European project itself at the security, political, democratic, economic and social levels. Accordingly, the EU understands that there is an urgent need to respond to this threat in order to protect its citizens, values, interests and also to reinforce its external credibility and responsibility to international peace and security.

CHAPTER 4

The Security Governance of Online Disinformation: the case of the European Union

The objective of this chapter is to introduce the security logic that the European Union uses to respond to online disinformation as a threat and the underlying reasons behind this logic. Therefore, it answers the following questions: *What sort of security logic was constructed by the European Union for the security issue of online disinformation, considering its understanding of the main elements that contribute to its proliferation and resilience? What prerequisites, goals and norms have the European Union discursively defined to address online disinformation as a threat to the foreign policy objectives in the eastern neighbourhood in terms of measures of denial and punishment? What prerequisites, goals and norms have the European Union discursively defined to address online disinformation as a hybrid threat to the European democratic, economic and social project in terms of measures of denial and punishment?*

Since 2015 that the European Union officially considers online disinformation as a threat. Yet, this understanding has been evolving, associated with the progressive complexity, multiple forms and effects underlying online disinformation. Consequently, the normative justification of the European Union to respond to disinformation has multiple rationales that produce different initiatives within the scope of the security governance. The progressive understanding concerning disinformation in security terms is demonstrated on how the European Union has come to discursively construct online disinformation as a threat, but also in the choice of words for presenting the initiatives to respond to this phenomenon. For instance, in the Communication from the European Commission on Tackling online disinformation: a European Approach the word to signal the response to disinformation at EU level was "approach". Whereas in the Joint Communication from the European Commission and the High Representative on the Action Plan against Disinformation, the words "action plan against" demonstrate more assertiveness.

Therefore, it is important to take into consideration that the response of the European Union to the threat of disinformation is not straightforward, has been adapting, and the evolving normative standing to address the threat of disinformation has implications for the development and implementation of the response, which involves multiple dimensions, structures and actors. Accordingly, the European Union understands that two elements must be considered. Firstly, it is important to distinguish between illegal content and content that is harmful, but not illegal. Secondly, the lack of deceiving and harmful intention or economic gain underlying misinformation should be met with actions that aim to raise awareness of the multiple actors of the society to this type of content and improve media and digital literacy. Whereas coordinated efforts underlying foreign interference in the information space and information influence operations reveal an intention to cause harm and are met with a more robust and holistic response. Hence, the European Union understands that a "calibrated response is needed from all parts of society, depending on the degree of harm, the intent, the form of dissemination, the actors involved and their origin" (European Commission and High Representative 2020c). Moreover, it is important to note that in the multiple initiatives presented by the European Union to respond to disinformation the full compliance with fundamental rights and democratic standards is always at the core of the action, confirming the preoccupation with proportionality in responding to online disinformation at EU level, in particular with the protection of fundamental freedoms such as freedom of expression[52].

In order to analyse the security governance of online disinformation at EU level, this study uses the concept of democratic deterrence introduced by Wigell (2021). This option results from the need to present a clearer and organised analysis of the main security logics underlying the security governance of online disinformation at EU level. But also, because the European Union understands that the calibrated response to interference and influence activities in the form of disinformation should involve initiatives to prevent successful manipulation – denial measures -, but also actions to impose costs – punishment measures. This is demonstrated in the Communication from the European Commission on Tackling online disinformation: a European Approach that acknowledges that tackling disinformation demands "collective resilience in support of our democratic bearings and European values" (2018a). Moreover, the Democracy Action Plan presented by the European Commission (2020a) reinforces the need to involve measures of denial as well as of punishment, thus the EU understands that actions should be taken to"…prevent the manipulative amplification of harmful content by increasing transparency, curbing manipulative techniques and reducing economic incentives for spreading

[52] At the EU level, the protection, respect, promotion of fundamental rights and freedoms is not directly specific. Nevertheless, it is possible to identify specific preoccupations as the response to online disinformation evolves. Firstly, in 2015, the fundamental rights and freedoms were more about the rights and freedoms of the citizens of the neighborhood countries (High Representative 2015); from 2018 onwards, the preoccupations have been more about European citizens and citizens of democracies (European Commission 2018a) and the COVID crisis was accompanied by the inclusion of the need to protect also the media, academia and civil society in particular (European Commission and High Representative 2020c).

disinformation, as well as introduce deterrence by imposing costs on actors engaged in influence operations and foreign interference".

The response of democracies to disinformation is complex considering the particular vulnerability of these regimes to this threat. On the one hand, the openness of democratic societies is fertile ground for actors with malicious and harmful intentions to interfere through covert, subtle and non-military means in the form of disinformation, aiming at undermining internal cohesion and affecting the decision-making process. On the other hand, there is a sense of urgency in democracies to find strategies, tools and instruments to respond to these challenges without jeopardizing the same values that are under threat (Wigell 2021, pp.49-50). In order to respond to this dilemma, Wigell (2021) proposes the concept of democratic deterrence. Wigell (2021) argues that the literature has mostly focused on the vulnerability underlying democracies and aims to demonstrate that "democracy itself is a potent strategic weapon" (p.50). Accordingly, liberal democratic values should not be limited to security vulnerabilities, but should also be considered as strengths to deter hybrid interference, particularly in the form of disinformation, and as instruments to build democracies that are more robust and resilient (*ibid* p.50).

The concept of democratic deterrence is based on five fundamental elements. The complexity and the transnational character of hybrid interference and disinformation represent challenges for an isolated response at the state level. Therefore, the development of resilience capabilities, the preparedness to respond and to ensure the realisation of vital societal activities should be defined and coordinated by the state, but supported by other societal actors. Hence, the first element underlying democratic deterrence refers to the agency and to the responsibility to act and respond to the threat of disinformation, that should be based on a whole-of-society approach, which, despite the coordination of the actions should remain with the state, it should involve the wider society (Wigell 2021, p.53).

The second element is related to the attraction rational underlying soft power. Accordingly, democratic principles and values are more than vulnerabilities, but mostly considered as strategic assets used to deter actors with malicious intent from interference (Wigell 2021, p.53).

Moreover, thirdly, the instruments used within the context of democratic deterrence are democratic and mostly non-military. Transparency, the rule of law and citizen activism are considered and used as tools to deter actors from interference. Accordingly, considering that hybrid interference flourishes through covert action, by means of transparency, namely through the identification and exposure of these campaigns, the subtle action that wanders under the radar is challenged. Furthermore, democratic societies based on a strong rule of law, translated into transparent and accountable governments and institutions, have the capabilities to deny the success of efforts to destabilise and sow internal distrust and discord. In addition, the involvement of citizens and civil society through citizen activism means that citizens are more aware and resistant to being deceived and consequently are also part of the efforts to expose these type of campaigns (Wigell 2021, p.54).

Fourthly, the principles and the values underlying democracy should be the answer and in no case should they be jeopardised. Hence, the need to address interference in the form of disinformation must take place without contradicting democratic norms and values, and avoid being seduced to respond through the same type of action. Accordingly, election meddling, corruption operations, disinformation campaigns and other instruments of sharp power should not be used, considering the paradoxical consequences associated with the peril of eroding liberal democratic values and normative legitimacy (Wigell 2021, p.54).

The fifth element assumes that the strategy of democratic deterrence is incapable to fully respond to the threat of interference. Furthermore, absolute deterrence is not even desirable, because it has the potential to encourage perpetrators to find alternative forms of interference actions, which may turn out to be more complex and dangerous (Wigell 2021, p.54).

Therefore, the ultimate objective of democratic deterrence is to develop and implement measures that increase the perceive costs of malicious and hostile interference to the point that outpaces its potential benefits. Moreover, the response should lie on the openness of democracies and avoid actions that potentially jeopardise democratic principles, norms and values in the name of security (Wigell 2021, p.55).

Democratic deterrence is based on actions of denial through resilience and of punishment through compellence. On the one hand, in order to deter through denial, actions are focused on the improvement of democratic resilience, by identifying and addressing the vulnerabilities underlying democratic states and societies, to make them less permeable to be influenced and manipulated. These actions involve the creation of an autonomous civil society, the increasing transparency of money flows and the broadening of inclusive politics. On the other hand, the improvement of democratic resilience should be the base of the democratic deterring action, however it is insufficient, thus demanding more assertive measures of punishment through compellence (Wigell 2021, pp.55-56).

In terms of measures to improve democratic resilience, civil society has a central role in the development of societal resilience. According to Hedling (2021), societal resilience is the ability of societies to resist and debunk disinformation claims and, thus, contribute to contain this type of threats (p.845). Hence, societal resilience refers to the efforts to raise awareness and empower civil society to resist to this type of actions and content, but it also refers to its involvement in the response and as part of the efforts to identify and expose this type of campaigns. Therefore, in order to enhance citizen activism, measures should focus on raising awareness, implementing rapid alert systems, media literacy programs and training of media professionals and journalists, aiming at identifying and exposing disinformation (Wigell 2021, p.55).

Democratic resilience also demands measures of transparency, particularly in relation to foreign interference and influence activities. In order to increase transparency in this context, actions should focus on the identification, analysis and exposure of disinformation campaigns and on raising public awareness to the existence of these activities. These measures aim to hamper the success of interference and influence activities, particularly in the form of disinformation, and disrupt any potential alliance between foreign aggressors and domestic actors. Moreover, the improvement of transparency in relation to money flows is of particular concern. Therefore, measures should be taken to identify sources of financing for political and social domestic actors with political and social influence, such as non-governmental organisations, political parties, the media and research institutions. In addition, the main vehicle for the dissemination of these campaigns is social media platforms, thus increasing transparency and implementing regulation, particularly in relation to political advertisement, is important to identify and delete sources of disinformation (Wigell 2021, pp.57-59).

The improvement of democratic resilience demands broaden inclusion, translated into societal security, based on the involvement of the whole society in the resilience-building process, in which citizens need to be aware of the existence of these activities and should have access to instruments that allow them to identify these campaigns. Therefore, measures should focus on enhancing education, social cohesion, welfare and also on amending electoral laws to consider the new dynamics underlying these old realities of interference in the information space (Wigell 2021, p.59).

Democracies acknowledge that they are not capable to fully respond to interference and influence activities such as disinformation campaigns through denial, thus requiring measures of punishment in the form of democratic compellence. Compellence is a strategy that aims to challenge the strategic calculus of the aggressor, traditionally through military actions or coercive diplomacy. Wigell (2021) considers that democracy can also be used as a form of compellence in response to authoritarian systems, considering its potential to challenge authoritarian control (p.60).

Wigell (2021) introduces certain premises that must be considered in order to successfully use democracy as an instrument of compellence. First, the use of democratic compellence as a strategy should take into consideration the communication of the thresholds underlying the response strategy. Accordingly, another form of transparency is the communication that certain unacceptable behaviours will have consequences and will be met with specific measures of punishment. Yet, in order to prevent jeopardising democratic liberal principles, these measures must not take place in the same domain of action as interference activities and should not be symmetrical (Wigell 2021, p.60).

Secondly, deterring through punishment may involve the implementation of sanctions. The use of sanctions as a deterring measure do not necessarily mean its actual application, it aims mostly to signal the will and preparedness to respond against previously communicated unacceptable behaviour. Today, the world is interdependent and interconnected, meaning that in order to maintain and improve security and economic progress states need to have access to the global flows of goods, resources, data and capital. These global flows still remain mostly controlled by western democracies, hence, by coordinating efforts and using well-calibrated sanctions and other policies of containment and engagement democracies can potentially challenge authoritarian regimes (Wigell 2021, p.61).

Thirdly, Wigell (2021) argues that democracy and democratic instruments and tools have the potential to be used as a vehicle of punishment, but should be used with prudence to avoid any potential escalation. In this context, the development and implementation of programs that promote democracy and human rights in the neighbourhood of authoritarian states can be used as democratic compellence. Accordingly, cultivating democratic principles and values through networks and proxies in the neighbourhood of authoritarian states by means of soft power and public diplomacy is considered to be a challenge to authoritarian states, because of the potential emergence of bottom-up democratising movements. The support to social and political activism by western liberal democracies creates a tricky choice for authoritarian regimes, between allowing those relations, risking deepen citizen activism or harden the pressure on civil society and further eroding legitimacy. Hence, signalling will and preparedness to support democracy, human rights and civil activism is a form of democratic compellence to defy autocracies. However, this type of action can be understood and exposed as an alternative form of interference and influence (Wigell 2021, pp.62-63). Nevertheless, Wigell (2021) considers that hybrid interference is different from the promotion of democracy and human rights. Whereas hybrid interference and influence are forms of covert manipulative interference, the promotion of democracy tends to be open, overt and transparent and thus considered as a form of legitimate public diplomacy that respects international legal standards. Yet, despite its legitimate action, the impact and effects underlying the promotion of democracy and human rights should not be overstated, because the response from authoritarian regimes to any dissent is likely to happen. Nonetheless, this type of democratic compellence has the potential to reinforce the objectives of democracies of exposing authoritarianism and boost their soft power (p.63).

To sum up, hybrid interference in the form of disinformation is not new, however, today, there is a widespread concern about its implications for democracies. The DNA of democracies makes them particularly vulnerable to this type of activities and the urgency to respond is challenged by its potential to jeopardise fundamental democratic values and principles. In order to overcome this dilemma, Wigell (2021) proposes the concept of democratic deterrence that understands democracy beyond a vulnerability. Accordingly, to successfully respond to hybrid interference democracies should implement measures that aim to improve democratic resilience. At the same time, democracies need to acknowledge that some actions of interference will be hard to deter and require a more assertive posture of punishment, namely by exposing interference actions, sanctioning and promoting democracy in the neighbourhood of authoritarian regimes (pp.63-64).

In this context, the European Union recognises the urgent need to respond to disinformation, through a proportional level of reaction in full compliance with fundamental rights and freedoms, by means that aim to improve the resilience of European democracies and measures that impose costs on actors engaged on interference operations in the form of disinformation (European Commission 2020a).

The next sub-chapter analyses the logics, the prerequisites, the goals and the norms underlying the security governance of online disinformation by means of democratic deterrence at EU level.

4.1. The Security Governance of Online Disinformation at EU level: deterrence by denial and punishment

The security governance of online disinformation at EU level is based on a strategy of democratic deterrence and involves measures of denial and punishment. In order to analyse the rational underlying this strategy it is important to consider how the European Union understands this threat, particularly in terms of what contributes to the proliferation and resilience of this type of content.

Initially, in 2015, the understanding of disinformation as a threat at EU level was mostly related to the role of communication tools in the political, economic and security developments in its eastern neighbourhood. Therefore, the response to disinformation was focused on denial measures in particular on improving strategic communication at EU level, considered an important tool in furthering the EU's policy objectives in the eastern neighbourhood. Accordingly, the development of positive and effective messages about the policies of the EU in the region, with the aim of allowing citizens to understand the positive impact of the political and economic reforms promoted by the EU, were the main actions taken to tackle disinformation. Moreover, those messages should also communicate the fundamental values promoted by the EU – democracy, the rule of law, the fight against corruption, minority rights and fundamental freedoms of expression and of the media. Hence, the actions underlying the Action Plan on Strategic Communication presented by the High Representative in 2015 were mostly based on measures of denial aiming at improving democratic resilience in the eastern neighbourhood region by means of strategic communication and by strengthening the media ecosystem. Nonetheless, measures of punishment were also implemented, with the objective of increasing the capacity of the EU to anticipate and respond to such activities, mostly through the identification and exposure of disinformation (High Representative 2015).

Therefore, in response to disinformation as a threat to the foreign policy objectives in the eastern neighbourhood the *prerequisites* were based on the *interest* of the European Union to challenge disinformation promoted by Russia and to protect the realisation of the EU's overall policy objectives in the eastern neighbourhood. This interest is in particular demonstrated in the European Council Conclusions of March 2015 that identifies the need to "challenge Russia's ongoing disinformation" and that invites the High Representative to prepare and present, in cooperation with member states and EU institutions, an Action Plan on Strategic Communication by June 2015 (European Council 2015).

Furthermore, the *goals* identified in the Action Plan on Strategic Communication to guide the initial response of the European Union to online disinformation, based on three main areas. First, to promote effective communication and EU policies and values towards the eastern neighbourhood. Second, to strengthen the overall media environment including the support for independent media. Third, to increase public awareness of disinformation activities by external actors and to improve EU capacity to anticipate and respond to such activities (High Representative 2015).

Moreover, the Action Plan underlined the *norms* that guided the response to online disinformation at the EU level, in particular the commitments with democracy, the rule of law, the fight against corruption, minority rights and fundamental freedoms of expression and of the media (High Representative 2015).

Today, the European Union understands online disinformation as a complex, multi-layered and evolving threat. Accordingly, the EU considers that online disinformation has multiple forms and interrelated causes and implications of economic, technological, political and ideological nature and is an evolving threat, demanding a comprehensive and coordinated response that continuously assess the relevant actors, vectors, tools, methods, targets and impact. Therefore, the complex and evolving nature of disinformation requires a comprehensive response and political determination, coordinated action and cooperation. The EU recognises that "addressing disinformation requires political determination and unified action, mobilizing all parts of governments...in close cooperation with like-minded partners across the globe…close cooperation between Union institutions, member states, civil society, the private sector, especially online platforms" (European Commission and High Representative 2018a). This is reinforced in the Joint Communication from the European Commission and the High Representative on Tackling COVID-19 disinformation-getting the facts right (2020c), which sets out a 'whole-of-society' approach and the need to strengthen the cooperation between public authorities, journalists, researchers, fact-checkers, online platforms and civil society.

In this context, the European Union understands that the spread and resilience of online disinformation is mostly linked to three main issues. Firstly, the EU considers that the dissemination of disinformation is both a cause and a symptom of a wider phenomenon related to the rapid change that societies are facing, economically, politically and culturally. Accordingly, there is a widespread sense of economic insecurity, rising extremism and cultural shifts that are generating anxiety and creating fertile ground for disinformation to spread and fuel societal tensions, polarisation and distrust. Therefore, the European Union considers that the response to disinformation should be based on clear political will to strengthen collective democratic resilience (European Commission 2018a).

Secondly, the European Union acknowledges the transformation in the media sector, particularly the impact of social media platforms on traditional journalism and on news media professionals, that are seeking to adapt their business models to the new reality of online news. Moreover, the EU also highlights that social media platforms have been taking a role usually associated with traditional media as content aggregators and distributors, but without the application of traditional editorial frameworks, with implications for the fact-checking of content that is disseminated. Hence, the European Union considers that there is a need to reinforce the role and quality of professional journalism and fact-checking (European Commission 2018a).

Thirdly, the European Union highlights the fundamental role that the manipulation of social media technologies has on the creation, amplification and dissemination of disinformation campaigns. Technologies now available are more affordable and intuitive in its usage, allowing the creation of false pictures and audio-visual content that are being use for deceiving purposes. Moreover, these new technologies, particularly social media have multiple mechanisms that enable the amplification of the proliferation of disinformation. The business model of social media platforms is algorithm-based and privileges personalised and sensational content because it is usually most likely to attract attention and to be shared among users. Furthermore, it is advertising-driven, which is mostly click-based and rewards sensational and viral content. In addition, multiple technological features of these platforms, such as automated services, usually referred to as ‘bots’, artificially amplify the dissemination of disinformation, which is then enhanced by fake accounts that sometimes work on a massive scale commonly known as troll factories. Consequently, the EU recognises that new technologies, particularly social media, have been used to disseminate disinformation and have so far failed to act proportionality and respond to the challenges posed by disinformation and the manipulation of these platforms (European Commission 2018a).

Furthermore, the EU acknowledges the role that the users of these platforms have in the dissemination process of disinformation campaigns, many times in the form of misinformation (European Commission 2018a). This preoccupation with users and citizens being part of the problem, and consequently of the solution, is reinforced in the Council of the European Union Conclusions on Media Literacy on 26th May 2020. The Council noted that the new media ecosystem, particular social media platforms, overwhelms citizens with information that consequently struggle to identify accurate information and reliable news sources. Thus, the Council foresees the need to implement media literacy initiatives that should not be limited to educate citizens about new technologies, but empower them with critical thinking skills to analyse complex realities and to distinguish the difference between opinion and facts (Council of the European Union 2020).

Therefore, the European Union assumes that no single solution is capable to address the threat of online disinformation and requires close cooperation between Union institutions, member states, civil society, researchers, fact-checkers, the media and the professional journalism sector, the private sector, with emphasis on social media, and with international like-minded partners. This is demonstrated in the initiatives to address the challenge of disinformation that involves multiple key areas, from the Communication on Tackling Online Disinformation and the Action Plan against Disinformation to the Communication on Increasing resilience and bolstering capabilities to address hybrid threats, on Securing free and fair elections, the European Democracy Action Plan, the EU's Cybersecurity Strategy for the Digital Decade, the EU Security Union Strategy, the Action Plan on Human Rights and Democracy, on Shaping Europe's digital future, the Strategic Compass and so on. Hence, disinformation at EU level is not only about disinformation, but also about security, democracy, human rights, economy, and so on.

Hence, in terms of the response to online disinformation as a hybrid threat to the European democratic, economic and social project the *prerequisites* are based on the *interest* of the European Union to protect and promote the European project itself at all levels.

The European Union understands that online disinformation is a challenge with multiple causes, forms and implications of economic, technological, political and ideological character that demands a comprehensive response. Therefore, the main *goals* defined by the European Union to act against disinformation can be summarised in four main objectives. Firstly, to improve transparency regarding the origin of information and the way it is produced, sponsored, disseminated and targeted, aiming at enabling citizens to assess the content they access online and to reveal possible attempts to manipulate opinion. Secondly, to promote diversity of information, aiming at enabling citizens to make informed decisions based on critical thinking, through support to high quality journalism, media literacy, and the rebalancing of the relations between information creators and distributors. Thirdly, to foster credibility of information, by providing an indication of its trustworthiness, notably with the help of trusted flaggers, and by improving traceability of information and authentication of influential information providers. Fourthly, to fashion inclusive solutions, because effective long-term solutions require awareness-raising, more media literacy, broad stakeholder involvement and the cooperation of public authorities, online platforms, advertisers, trusted flaggers, journalists and media groups (European Commission 2018a).

In terms of the *norms* that guide the response to online disinformation, the universal values promoted by the EU, particularly the commitment to democracy, remain the most important. Nevertheless, the European Union particularly highlights the need to protect freedom of expression within the framework of the response to disinformation. This preoccupation is particularly demonstrated in the evolution from the Communication from the European Commission on Tackling online disinformation: a European Approach to the Joint Communication from the European Commission and the High Representative on the Action

Plan against Disinformation. Whereas the former starts by making the point that disinformation is a threat, the later starts by making the point on the need to protect fundamental democratic values and principles with emphasis on freedom of expression. Hence, more than responding to disinformation, the fundamental objective is the protection of freedom of expression, reinforced in the Guidance on Strengthening the Code of Practice "…the EU approach to countering disinformation has been grounded in the protection of freedom of expression…rather than criminalising or prohibiting disinformation as such", which confirms the preoccupation with a proportional level of reaction and moral authority to respond namely in terms of protecting fundamental rights and freedoms (European Commission 2021b).

In conclusion, the security governance of online disinformation at EU level is based on a strategy of democratic deterrence that involves measures of denial, that aim to improve democratic resilience in order to prevent the successful use of manipulation, and also measures of punishment by exposing disinformation campaigns and imposing costs and thus challenging the strategic calculus of actors engaged in interference operations in the form of disinformation. Moreover, it involves a whole-of-society approach aiming at protecting the European project in all aspects. This results from the understanding of online disinformation as a complex, multi-layered and evolving threat that has interrelated causes and implications of economic, technological, political and ideological nature. But also, the understanding of online disinformation as an evolving threat, that demands a comprehensive and coordinated response that continuously assess the relevant actors, vectors, tools, methods, targets and impact. At the same time, coordinated efforts to interfere in the form of disinformation are met with a more robust approach, whereas the dissemination of false or misleading content without intention is addressed mostly through actions of awareness and media literacy. Therefore, there is a widespread preoccupation with a calibrated response to online disinformation that must be in full compliance with fundamental rights and freedoms in particular with freedom of expression, manifesting a concern with proportional action.

In order to better understand the operationalisation of this strategy and the proportionality underlying the level of reaction of the European Union to online disinformation, the next chapter does a descriptive analysis of the *structures*, initiatives and actors, involved in the implementation of the strategy of democratic deterrence to respond to online disinformation at EU level.

CHAPTER 5

Deterring Online Disinformation through denial: the case of the European Union

The objective of this chapter is to analyse descriptively the *structures*, the main initiatives and the actors, involved in the security governance of online disinformation at EU level through democratic deterrence, in particular through measures of denial. Nevertheless, it is important to note that although we analyse first the denial measures and in the next chapter the measures related to punishment initiatives, this does not mean that the implementation of this strategy occurs separately and that the actors only engage in one type of action. Moreover, despite our analysis firstly considers the actions taken to respond to online disinformation as a threat to the foreign policy objectives in the eastern neighbourhood and later on the actions taken to respond to online disinformation as a hybrid threat to the European democratic, economic and social project that does not mean that one approach ended to start the other, as we will demonstrate in the next chapter, but this option aims to organise the analysis.

Hence, by analysing the *structures* involved in the response to online disinformation this chapter contributes to the analysis concerning the proportionality in the level of reaction of the European Union to online disinformation through measures of denial. In this context, it is important to note that the EU understands that under the principle of proportionality "the content and form of Union action shall not exceed what is necessary to achieve the objectives" (Article 5 of the Treaty on European Union). Considering this, this chapter answers the following questions: *What structures of security governance have resulted from constructing online disinformation as a threat? What denial initiatives have been defined by the European Union to respond to disinformation as a threat to the foreign policy objectives in the eastern neighbourhood? Which actors are involved in these structures? What denial initiatives have been defined by the European Union to respond to disinformation as a hybrid threat to the European democratic, economic and social project? Which actors are involved in these structures?*

5.1. Deterring Online Disinformation as a threat to the foreign policy objectives in the eastern neighbourhood through denial

The *structures* design to challenge disinformation promoted by Russia and to protect the realisation of the EU's overall policy objectives in the eastern neighbourhood were mostly based on denial initiatives aiming to improve democratic resilience in the eastern neighbourhood region through strategic communication and support for the media ecosystem. Therefore, the High Representative proposed that the initial action to challenge disinformation should focus on firstly, increasing the strategic communication capacity of the European Union. Secondly, on cooperating with partners and developing networks. Thirdly, on investing in communication activities on EU funded programs, projects and activities in the eastern neighbourhood. Fourthly, on supporting freedom of the media and freedom of expression. Fifthly, on implementing public diplomacy initiatives in the neighbourhood. Sixthly, on improving capacity building for journalists and media actors. Seventhly, on supporting pluralism in the Russian language media space. Eighthly, on engaging with civil society, that will be further discussed in the next chapter in term of punishment measures. Ninthly, on increasing awareness, developing critical thinking and promoting media literacy. Tenthly, on strengthening the cooperation on regulatory issues in EU member states. Accordingly, initially, the main actors involved in operationalising denial actions to tackle disinformation as a threat to the foreign policy objectives of the European Union in the eastern neighbourhood were the High Representative, the European External Action Service, particularly through the East StratCom Task Force, and the member states. Moreover, other EU institutions, organisms and delegations, external partners, like-minded third countries, regional and international organisations, journalists and media representatives, and civil society have been also part of the efforts to respond to disinformation in the eastern neighbourhood (High Representative 2015).

The operationalisation of these objectives, particularly the increasement of the EU strategic communication capacity and the increasement of awareness, development of critical thinking and promotion of media literacy have been the responsibility of the East StratCom Task Force, set up in the Strategic Communications and Information Analysis Division of the European External Action Service with three main tasks. First, the Task Force is responsible for producing communication products and campaigns that explain EU values, interests and policies in the Eastern Partnership countries[53]. Second, the Task Force should also support efforts to strengthening the media landscape in the Eastern Partnership countries. Third, the Task Force should also identify and analyse disinformation trends. Moreover, it should report and expose

[53] Eastern Partnership countries are: Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova and Ukraine.

disinformation narratives and raise awareness for their existence and negative impact, a task that is part of the punishment measures[54].

Furthermore, in order to improve the impact and the effectiveness of the communicational actions, the European Union highlights the importance of cooperation and the development of networks. The Action Plan presented by the High Representative identifies four levels concerning the networks. First, at the EU level, networks should be created between EU institutions, delegations, member states, in order to improve coordination and coherence of the European messaging to the eastern neighbourhood. Second, networks should also be built with external partners, like-minded third countries, regional and international organisations. Third, the creation of networks should also include journalists and media representatives, to support independent media, but also to assist the effectiveness of communication of EU policies. Fourth, networks should also be done with civil society actors, to support public awareness actions that aim to expose the existence of this type of activities and to educate on how to react to it (High Representative 2015).

Moreover, the European Union also recognises the added value of investing in communication activities through other ongoing communicational programs, projects and activities carried out by EU delegations and member states embassies in the eastern neighbourhood, such as the regional communication programme "EU's Neighbourhood Communication Programme", which includes EU NEIGHBOURS east and south[55] (High Representative 2015).

The European Union also understands that to improve its communication in the eastern neighbourhood, to be closer to local populations and to be capable to effectively explain its policies, promote dialogue and ensure that citizens are informed properly about the EU, it needs to implement public diplomacy initiatives that involves the engagement with local populations, namely the youth, academia and civil society. These initiatives are implemented through the Partnership Instrument, Jean Monnet Programme and Erasmus Plus. Moreover, the Action Plan also considers the importance of producing communication materials in local languages, particularly in Russian, in order to promote pluralism in the Russian language media space and provide information in local languages from different sources other than Russian (High Representative 2015).

[54] For a deeper understanding of the work of the East StratCom Task Force see https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11233.

[55] For a deeper understanding of this Programme see, for instance, https://euneighbours.eu/.

In terms of strengthening the overall media environment, the European Union recognises that media policy is a national competence, but cooperation between national regulators is essential, particularly considering the cross-border nature of disinformation. Moreover, in relation to the support of freedom of the media and freedom of expression, the EU and its member states will continue to actively engage through its cooperation and support to the activities of the Organization for Security and Co-operation in Europe (OSCE) and the Council of Europe. Furthermore, it will work closely with Eastern Partnership countries, particularly with Ukraine, Moldova and Georgia on the implementation of important issues of the Association Agendas concerning the freedom of expression, assembly and association (High Representative 2015).

In conclusion, we argue that the initial response of the European Union to disinformation promoted by Russia in the eastern neighbourhood was proportional, mostly focused on initiatives of denial by improving the strategic communication of the EU in the region and thus not exceeding the necessary actions to improve democratic resilience in the eastern neighbourhood and protect the realisation of the EU's overall policy objectives in the region.

5.2. Deterring Online Disinformation as a hybrid threat to the European democratic, economic and social project through denial

The *structures* design to protect the European democratic, economic and social project from hybrid threats in the form of online disinformation are based on four pillars of action, mostly dedicated to denial initiatives that aim to improve democratic resilience and prevent the success of manipulation. First, in order to respond to online disinformation, the European Union aims to improve the capabilities of Union institutions to detect, analyse and expose disinformation, that will be further discussed in the next chapter. Second, the EU aims to strengthen coordinated and joint responses to disinformation. Third, the EU aims to mobilise the private sector to tackle disinformation. Fourth, the EU aims to raise awareness and improve societal resilience (European Commission and High Representative 2018a).

At the same time, it is important to note that in terms of the actions to respond to online disinformation and protect the European project, the European Union continuously underlines its preoccupation of responding effectively to disinformation without jeopardizing fundamental rights and freedoms, in particular freedom of expression. The Democracy Action Plan (2020a) demonstrates this concern by emphasizing that "[the actions] cannot interfere with people's right to express opinions or to restrict access to legal content…" (European Commission 2020a). Therefore, since its inception that the response of the European Union to online disinformation considers the need to be proportional, particular in terms of protecting freedom of expression, and to not exceed beyond necessary to achieve the objectives. This is particularly demonstrated by the actions implemented that mostly aim to improve democratic resilience through public awareness, quality journalism and transparency of the online environment.

Therefore, in terms of the denial actions to respond to disinformation, firstly, the European Union considers that initiatives to increase public awareness and critical thinking are fundamental to develop critical analysis and digital competences, in both formal and non-formal education, to prevent the manipulative amplification of harmful content, to empower citizen participation in the economic, social, political and cultural aspects of society and democratic life, and thus to reinforce the resilience of societies to disinformation (European Commission 2018a). Accordingly, the European Union understands that to achieve this there is a need to foster education and media literacy; to support for free, independent media and quality journalism as an essential element of democratic society; and to secure and improve the resilience in the election process (European Commission and High Representative 2018a).

The European Union considers that the users of social media are one of the main factors that contribute to the amplification of the dissemination of disinformation, which in combination with the present political and economic context creates fertile ground for disinformation to spread and to become more resilient (Council of the European Union 2016). Consequently, the EU recognises that actions to foster education, media and digital literacy[56] are of utmost importance to improve democratic resilience and are operationalised through the support to new innovative projects to fight disinformation, namely developed by civil society organisations and higher education institutions with the involvement of journalists; through the support and funding for and diversifying initiatives to promote medial literacy and digital literacy, in order to capacitate citizens to identify disinformation within the EU and beyond and to participate in the online environment informed, wisely, safely and ethically (European Commission 2020a). Yet, as we further discuss in the next chapter, despite the added value of

[56] The European Union understands that media and digital literacy refers to "all the technical, cognitive, social, civic and creative capabilities that allow us to access and have a critical understanding of and interact with both traditional and new forms of media". This understanding includes different types of media, broadcasting, video, radio, press, and the various channels of media, traditional, internet, social media, thus the critical understanding and use of Information and Communication Technologies is also considered (Council of the European Union 2016).

educating citizens to access and critically analyse information, there are challenges related to psychological biases that may limit the success of this type of action.

Moreover, the European Union highlights that freedom of expression and freedom of the media are fundamental building blocks of the European project, this is particularly linked to the assumption that a healthy democracy is based on the active engagement of its citizens that should make a free and informed participation in the democratic life. Besides other sources of information, this informed participation rests mostly on an independent, free, pluralistic, accurate and with quality journalism. Nevertheless, the European Union understands that today one of the main causes and dynamics that enables the proliferation of disinformation relates to the transformation in the media ecosystem. The new media ecosystem involves traditional media, but also and with a growing participation new media with emphasis on social media. This new reality of social media has been accompanied by citizens being overwhelmed with information and challenge to find accurate information, reliable sources and quality content, and consequently being more potentially exposed to disinformation (Council of the European Union 2020). Therefore, raising awareness and improving societal resilience also demands the development and implementation of measures that support independent, free, pluralistic media and quality journalism. Accordingly, the European Union highlights the need to support quality journalism, to ensure a pluralistic and diverse media environment, that can uncover, counterbalance and dilute disinformation; to invest in high quality journalism and encourage quality news media to explore innovative forms of journalism, in order to reinforce trust in the role of professional journalism, online and offline, and provide quality and diverse sources of information to citizens; to rebalance the relation between traditional media and online platforms; to improve public support to media and public service media (European Commission 2018a). Hence, strengthening the European media ecosystem through the support for quality journalism is important "to secure sustainable production and visibility of professional journalism as a mean to empower citizens, protect democracy and effectively counter the spread of disinformation" (Council of the European Union 2018).

In addition, the European Union understands in its Democracy Action Plan (European Commission 2020a) presented by the European Commission that there is the need to support free, independent and pluralistic media in the response against disinformation, but it is also important to protect the safety of journalists which can be victims of abuses in the name of the fight against disinformation. Nevertheless, despite these important measures in support of quality in professional journalism there is little attention at EU level to the challenges related to traditional media being sources and vehicles for the proliferation of disinformation as identified in chapter two. This study does not aim to analyse and understand the causes behind this, but it can be useful for further research to understand why this happens and its implications.

Furthermore, the Action Plan against Disinformation (European Commission and High Representative and 2018a) also highlights the need from member states, in cooperation with the European Commission, to support the creation of a multidisciplinary community of independent fact-checkers, academic researchers and other relevant stakeholders that investigate disinformation. This is of particular importance to enhance the knowledge on disinformation, particularly to better understand the sources, the intentions, the tools, the objectives underlying these campaigns, and the internal vulnerabilities of the European Union and its member states to it, and consequently improve the capabilities on detecting, analysing, exposing and responding to disinformation. Hence, in order to facilitate the creation of this community and its activities, the European Commission and the High Representative propose in the Action Plan against Disinformation the establishment of the European Digital Media Observatory (EDMO) with the aim of supporting the independent community of fact-checkers, academic researchers and other relevant stakeholders that investigate disinformation and that work to combat disinformation. EDMO has five main tasks, first, to map fact-checking organisations in Europe and support them by fostering joint and cross-border activities and dedicated training modules. Second, to map, support and coordinate research activities on disinformation at EU level. Third, to create a public portal that provides media practitioners, teachers and citizens with information and materials aimed at increasing awareness, building resilience to online disinformation and supporting media literacy campaigns. Fourth, to design a framework to ensure secure and privacy-protected access to platforms' data for academic researchers working to better understand disinformation. Fifth, to support public authorities in the monitoring of the policies put in place by online platforms to limit the spread and the impact of disinformation[57].

Moreover, the EU understands that the support to the fact-checking and research community is mostly done through investing in research, hence the European Commission should finance, under the Europe Facility Programme, a digital platform that sustains a digital network for cooperation between independent national multidisciplinary teams of independent fact-checkers and researchers; the Commission also proposes funding for the development of

[57] To better understand the objectives, the tasks and the governance of this organism see https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory.

new tools to better understand and combat online disinformation in its proposal for Horizon Europe Programme (European Commission and High Representative 2018a).

Another element fundamental to improve democratic resilience is the promotion of free and fair elections. Accordingly, the European Commission assumes that the security of the electoral process as the basis of democracy is of particular concern. In this context, the use of disinformation has the potential to impact public debates and the formation of opinion, and it can also compromise the electoral process itself, for instance through false information about the schedules and the places to vote. At the same time, it is challenging to prevent timely detection of disinformation and implement a response. Therefore, the 2019 European Parliament elections triggered the action of the European Union towards disinformation in the context of the electoral process. The European Commission encouraged the competent national authorities to identify best practices for the identification, mitigation and management of risks to the electoral process form cyberattacks and disinformation. Moreover, the Commission proposes a continuous dialogue to support member states in the management of risks to the democratic electoral process associated with cyber-threats such as cyber-attacks and disinformation (European Commission 2018a). Furthermore, in the context of the Action Plan and the 2019 European elections, the European Commission and the High Representative also highlight the need for member states to ensure the follow-up of the Elections Package set up in 2018 (European Commission and High Representative 2018a)[58].

Secondly, the European Union acknowledges the fundamental role of strengthening coordinated and joint responses to disinformation and of the cooperation with international partners. In this context, the European Commission and the High Representative created a Rapid Alert System. This system provides alerts on disinformation campaigns in real-time through a dedicated technological infrastructure and facilitates sharing of data and assessments, in order to enable common situational awareness, coordinated attribution and response and to ensure time and resource efficiency. In this context, each member states designates, in line with its institutional setup, a contact point, ideally positioned within strategic communications departments. This contact point shares alerts and ensures coordination with other relevant national authorities and with the European Commission and the European External Action Service. This Rapid Alert System should also be linked to the Emergency Response Coordination Centre and the Situation Room of the EEAS, and other actors as the EU Hybrid

[58] In order to better understand the actions of the European Union towards disinformation in terms of the electoral process see the Communication from the European Commission on Securing free and fair European elections and the European Democracy Action Plan.

Fusion Cell. Moreover, regular exchange of information and best practices should also occur with key international partners within the G7 and the North Atlantic Treaty Organisation (European Commission and High Representative 2018a).

Thirdly, the European Union considers the mobilisation of the private sector fundamental for improving democratic resilience in the response against online disinformation, particular in terms of creating a transparent, trustworthy and accountable online ecosystem. On the one hand, the EU recognises the important and positive role of the Internet, particularly with regard to the availability of information, in volume and diversity, that has changed how individuals access and engage with information, with potential to make the democratic process more participatory and inclusive. Nevertheless, on the other hand, the Union also acknowledges the negative and threatening use of new technologies, particularly social media, to create, amplify and disseminate disinformation on an unprecedent scale, speed and precision. At the same time, the European Union highlights that social media has been used as a vehicle to spread disinformation and have had a limited response to act proportionality and effectively in terms of the challenges posed by disinformation (European Commission 2018a). Moreover, according to Schia and Gjesvik (2020), global digital platforms have been gaining power and influence, particularly in terms of decisions concerning the sharing of information and content, without direct involvement of societies. Consequently, their increasing role in decision making about the sharing of content has the potential, if not closely monitored, to result in measures that control and block selectively information, thus denying public access to the narrative projected by the 'other', which goes in direct opposition to democratic principles and values (pp.3-4). Consequently, challenging the protection of fundamental rights and freedoms such as the freedom of expression.

This position of distrust towards the private sector at EU level is novel and has been mainly associated with the understanding that some actors from the private sector, particularly social media, have been unable or unwilling to address the challenges associated with disinformation. Ergo, the emergence of online disinformation as a threat has been accompanied by a re-assessment of trust associated with the cooperative relation between the European Union and the private sector. Accordingly, there has been a discursive shift underlying the relationship between the EU and the private sector, namely with the tech sector and with particular emphasis on social media platforms, which today require greater oversight in the perspective of the EU (Carrapiço and Farrand 2021, p.1161; Carrapiço and Farrand 2020, p.1111).

As far as it concerns the governance of cybersecurity, the European Union considers the private sector an important partner, because of its expertise and aligned interests in this security area. However, certain actors of the technological sector, particularly social media platforms, have been perceived suspiciously at EU level. This ideational shift in the relationship between the EU and some actors from the private sector, particularly social media, occurred between 2016 and 2019, associated with the discursive construction of disinformation in security terms and the key role of social media as a vehicle for its dissemination. Accordingly, the European Union considers that social media platforms have been contributing to the creation, amplification and spread of disinformation, yet these platforms have refused to assumed their responsibility to address this challenge, and have been consequently considered by the European Union as part of the problem. Hence, the EU recognises the important role of the actors from the private sector in providing security and economic growth to the Union space, but acknowledges that some are more reliable than others and are more in line with EU's fundamental values and principles. EU policymakers hold the perception that some social media platforms do not share the same values of the European Union and thus are less reliable. Whereas social media platforms, such as Facebook, assume that the plurality of views should be represented, whether being true or false, the European Union understands that this potentially contributes to the spread of deceiving and harmful content. For instance, the spread of disinformation campaigns by anti-vaxxers groups about contemporary vaccination, enabled by this principle of plurality of opinion promoted by social media platforms, has been accompanied by an increase of certain transmissible diseases. Consequently, the EU's understanding about the role of some actors from the private sector in the promotion and protection of democracy and democratic values and principles has been subjected to a reorientation, "whereas some private actors are trusted partners in cybersecurity, and believed to share the values of the EU, social media platforms are increasingly framed as being part of the problem, [and] not sharing those same values" (Carrapiço and Farrand 2020, pp.1117-1119, 1122).

This discursive reorientation concerning the relation between the European Union and the private sector was translated at the policy level through a distinction between actors that are trusted and part of the solution and actors that are less trusted and are not at the centre of the policymaking and the governance network, but are considered as agents in need of regulation (Carrapiço and Farrand 2020, pp.1117-1119, 1122).

Consequently, the European Commission in its Communication on Tackling online disinformation introduced the creation of the Code of Practice on Disinformation as a self-regulating voluntary piece that aims to mobilise the private sector to protect users from disinformation and to build a more transparent, trustworthy and accountable online ecosystem. Accordingly, the European Union understands that it is fundamental to involve the private sector in the response against disinformation, in order to promote adequate changes in platforms' conduct; to promote a more accountable information ecosystem; to enhance fact-checking capabilities and collective knowledge on disinformation; and to use new technologies to improve the way information is produced and disseminated online (European Commission 2018a).

The creation of the Code was based on one report presented by the High-Level Expert Group on fake news and online disinformation, that was created by the European Commission in January 2018 to advise the Commission on understanding the phenomenon of fake news and online disinformation and to set up a governance framework to respond to this type of content. The Code was formalised in October 2018 as a self-regulatory and voluntary instrument aiming at introducing a structured framework for monitoring and improving the policies of online platforms on disinformation, and as an instrument for major online platforms, providers of software, advertisers and trade associations representing online platforms and the advertising sector to compromise to identify actions to ensure greater transparency and accountability of their platforms (European Commission and High Representative 2018a). Furthermore, the Code also demonstrates the preoccupation of the European Union concerning the need to continuously assess the evolution of disinformation as a threat and the implementation of the commitments agreed in the Code by the Signatories, because this Code is followed by continuous assessments of its effectiveness to regularly analyse its implementation, progress, and functioning (European Commission and High Representative 2018a).

Therefore, the Code is an innovative tool created by the European Commission as part of the efforts to address the challenges posed by the dissemination of disinformation, set up with the aim of ensuring greater transparency, trustworthiness and accountability of the online ecosystem and as a framework for monitoring and improving policies in this regard. Accordingly, the main commitments of the Code aim to address the scrutiny of ad placements in the services of the Signatories; the transparency of political advertising and issue-based advertising in the services of the Signatories; the integrity of the services of the Signatories; the empowerment of consumers; and the empowerment of the research community (European Union 2018).

Nevertheless, the COVID-19 pandemic crisis emerged as a test to the effectiveness of the Code that proved to be limited, consequently creating the need for its reinforcement. The pandemic crisis has accelerated ongoing trends in terms of cyber-threats and cybersecurity and also in terms of the increasing use of online disinformation. Consequently, the challenges associated with cyberspace particularly in terms of disinformation were accompanied by more assertiveness in terms of regulation of digital platforms in general and social media in particular (Carrapiço and Farrand 2020, p.1111).

The European Commission recognised that the COVID-19 pandemic crisis reinforced the growing widespread dependency of states and societies on cyberspace and digital technologies, consequently contributing to an increase in vulnerability that has been exploited by malicious and hostile actors for political and economic purposes. In this context, the Commission acknowledged that online platforms have been used to spread disinformation associated with the pandemic and the risks that infodemic and particularly in the form of disinformation has for personal health, public health systems, effective crisis management, the economy and social cohesion demands a more urgent and robust action in terms of ensuring a safer online ecosystem. Accordingly, in response to the Report Assessment of the European Commission 2020, the Conclusions of the European Council December 2020, the Evaluation of the European Parliamentary Elections 2019 and the Joint Communication from the European Commission and the High Representative on Tackling COVID-19, the European Commission issued a Guidance on Strengthening the Code of Practice (European Commission 2021b).

In this context, the Report Assessment has revealed multiple and significant shortcomings in terms of the implementation of the Code by the Signatories. These shortcomings included inconsistent and incomplete implementation of the Code by online platforms and member states, that the European Union assumes as a result from the intrinsic limitations of the self-regulatory nature of the Code, from gaps in the coverage of the Code's commitments and from the absence of an appropriate and effective monitoring mechanism. In particular, the Report identified failures in terms of the quality of the monitoring and reporting process, especially concerning the inclusion of key performance indicators that are adequate and sufficient detailed, and also in terms of the absence of independent assessment. Moreover, the lack of sufficient fact-checking in the online services of the Signatories and the continued monetisation of disinformation are also major shortcomings related to the implementation of the Code (European Commission 2021b).

Therefore, the pandemic crisis not only reinforced the need to tackle online disinformation, but it particularly highlighted the need to reinforce the role of social media platforms. Accordingly, Carrapiço and Farrand (2020) argue that the pandemic demonstrated that social media platforms not only have a limited contribution to the definition and implementation of cybersecurity policies that prevent the dissemination of disinformation campaigns, they are in fact hinder the efforts to tackle it by continuing to allow its proliferation (p.1123).

Hence, social media platforms have come to be seen by the European Union mostly as part of the problem and in need of greater oversight, consequently the European Commission introduced in the Democracy Action Plan (2020a) the need for a Guidance on Strengthening the Code of Practice with the aim of reinforcing the commitments of the Signatories and to introduce measures that platforms and other relevant stakeholders should implement to address the shortcomings and the gaps identified in the Report Assessment (2020d) and contribute to create a more transparent, trustworthy and safer online environment. Accordingly, the European Commission highlighted the urgent need to demonetise disinformation; to upgrade commitments to limit manipulative behaviour, to strengthen tools that empower users, to increase transparency of political advertising, and to support the research and fact-checking community; to improve the framework to monitor the strengthened Code; to broaden the participation in the Code. Furthermore, the Guidance also aims to evolve the existing Code of Practice towards 'Code of Conduct'. Hence, the European Commission aims to strengthen the Code and create a stronger, more stable and more flexible instrument that makes online platforms more transparent, accountable and responsible by design. To this end, the strengthened Code seek to reinforce commitments, expand the scope, broaden the participation and tailor commitments (European Commission 2021b).

As far as it concerns the reinforcement of the commitments, the European Commission acknowledges that the use of disinformation is continuously evolving and new risks are quickly emerging. At the same time, the Code of Practice has not been sufficiently effective in providing a comprehensive response to these rapidly changing dynamics, demanding stronger and more specific commitments in all areas that address these shortcomings and achieve the objectives of the Code of tackling disinformation. Thus, the Commission proposes the creation of a permanent mechanism to continuously assess the progress of disinformation and the consequent regular adaptation of the Code (European Commission 2021b).

Moreover, the European Commission recognised that the 'infodemic' associated with the COVID-19 pandemic crisis demonstrated that the viral spread of false and misleading content with no malicious intention has also the potential to cause public harm. Hence, the European Commission highlighted the need to expand the scope concerning the challenges associated with disinformation to also include content such as misinformation (European Commission 2021b). Accordingly, the European Commission and the High Representative acknowledged in the Joint Communication on Tackling COVID-19 disinformation the need to clarify and distinguish different forms of false and misleading content that has the potential to do public harm, and the need to develop a calibrated response that is appropriate and proportional to the type of content (European Commission and High Representative 2020c). Therefore, the strengthened Code considers the risks and challenges posed by misinformation and commit Signatories to implement appropriate policies and proportionate actions to address it when significant public harm is at stake. This should occur without hampering the realisation of freedom of expression and mostly through measures that empowers users with access to authoritative sources and transparency measures that inform users that the information that they are seeing is verifiable false (European Commission 2021b). Reinforcing the discursive preoccupation of the European Union to respond to disinformation in an appropriate and proportional manner.

Furthermore, the Code is signed by major online platforms operating in the European Union such as META and Google. Yet, the increasing complexity underlying disinformation creates the necessity for the European Commission to propose the inclusion of more Signatories, established and emerging platforms, with particular focus on small online platforms, private messaging services and other relevant stakeholder from the advertising ecosystem (European Commission 2021b).

The strengthened Code aims to increase the impact on the demonetisation of disinformation, a critical area identified in the Report Assessment 2020. Therefore, the European Commission acknowledges the relevance of a broader participation of the advertising ecosystem and of other actors from the online advertising sector, such as brands, in particular those with substantial advertisement spending, and other participants involved in ad exchanges, ad-technology providers, communication agencies, and other players that provide services that may potentially be used to monetise with disinformation (e.g. e-payment services, e-commerce platforms, crowdfunding/donation systems) (European Commission 2021b).

In addition, the European Commission recognises that platforms for private messaging services can also be used to spread disinformation, thus they should also integrate the Code and commit to measures appropriate for their type of service, without undermining the encryption used in this type of services and without hampering the protection of privacy of its users (European Commission 2021b).

Moreover, the broaden participation in the Code may also include other stakeholders that can have a significant impact in the response to disinformation, because of their tools, instruments, solutions or relevant expertise, including fact-checkers, organisations providing ratings relating to disinformation sites or assessing disinformation, as well as providers of technological solutions to support the efforts to tackle the challenges related to the dissemination of disinformation (European Commission 2021b).

At the same time, the European Commission recognises that the relevant compliance burdens, including reporting obligations commitments should be proportional and consider the size of the services of the Signatories. Accordingly, whereas major online platforms should commit to more robust measures, smaller and emerging platforms should not be subject to disproportionate burden (European Commission 2021b).

Additionally, the European Commission considers the diversity of services provided by the Signatories of the Code and proposes tailored commitments that correspond to the roles and services that the Signatories have in the digital ecosystem. Accordingly, Signatories should commit to actions relevant and appropriate for their services to facilitate a broader and effective participation (European Commission 2021b).

The Report Assessment 2020 also identified the lack of sufficient fact-checking in the online services of the Signatories, hence the strengthened Code considers the relevance of involving fact-checking expertise. Therefore, the European Commission proposed the creation of a multidisciplinary community of fact-checkers, academic researchers and other relevant stakeholders to support the increase of capacity to detect and analyse disinformation campaigns in the online services of the Signatories (European Commission 2021b).

The strengthened Code is also committed with improving cooperation and exchanging of information and timely alerts, thus the European Commission highlights the need to reinforce the cooperation between the Signatories and the EU Rapid Alert System, which connects all EU member states and relevant EU institutions to enable joint responses to disinformation through information sharing and by providing timely alerts (European Commission 2021b).

The Signatories of the Code of Practice committed in 2018 to implement actions to address the scrutiny of ad placements; political advertising and issue-based advertising; the integrity of their services; the empowerment of users; and the empowerment of the research community. The strengthened Code proposes more detailed and robust commitments in these areas.

As far as it concerns the scrutiny of ad placements, the European Commission highlights the need to increase the efforts and the impact of the Code on demonetising the purveyors of disinformation. Hence, the European Commission recognises the need for the strengthened Code to commit to more granular and tailored actions to address disinformation risks related to the distribution of online advertising. Therefore, the European Commission proposes actions that aim to address the demonetising of disinformation, to improve cooperation between relevant players and to implement commitments to address advertising containing disinformation (European Commission 2021b).

In terms of the demonetising of disinformation, the Code aims to defund the dissemination of disinformation by means of improving the transparency and accountability underlying ad placements. Therefore, Relevant Signatories[59] commit to improve policies and systems which determine the eligibility of content to be monetise; to improve the controls for monetisation and ad placements; and to improve the data to report on the accuracy and effectiveness of controls and services around ad placements (European Union 2022b).

Moreover, in order to improve the effectiveness of scrutiny of ad placements and demonetise disinformation, the European Union considers fundamental the broaden participation and inclusion of the online advertising ecosystem and the increased cooperation between all participants and the creation of cross-industry initiatives aiming to facilitate the exchange of best practices, information on disinformation ads refused by one platform to prevent their appearance on other platforms (European Commission 2021b). Thus, Relevant Signatories commit to exchange best practices and strengthen cooperation with relevant players, expanding to organisations active in the online monetisation value chain, such as online e-payment services, e-commerce platforms and relevant crowd-funding donation systems (European Union 2022b).

Furthermore, the European Commission highlights the need to address the misuse of advertising systems for spreading disinformation and to implement transparency policies to explain advertisers which advertising policies have been violated when ads have been rejected or removed or accounts disabled. To this end, Relevant Signatories commit to prevent the misuse of advertising systems to disseminate disinformation in the form of advertising messages (European Union 2022; European Commission 2021b).

With regard to the commitments concerning political advertising[60] and issue-based advertising[61], the European Commission highlights the role of this type of advertising in shaping political campaigns and public debates, and its potential impact in the formation of public opinion and in the outcome of elections, therefore there is a need to ensure an adequate level of transparency and accountability in this type of advertising (European Commission

[59] Relevant Signatories refers to the individual Signatory that has accepted certain commitments relevant and appropriate for their services according to a given area of the Code.

[60] The European Union understands political advertisement as "advertisements advocating for or against the election of a candidate or passage of referenda in national and European elections" (European Union 2018).

[61] The European Commission understands issue-based ads as ads that include sponsored content on societal issues or issues related to a debate of general interest that might have an impact on public discourse, such as the COVID-19 pandemic crisis, migration, environment (European Commission 2021b).

2021b). Therefore, firstly, Relevant Signatories commit to adopt a common definition of political and issue advertising. Secondly, Relevant Signatories commit to apply a consistent approach across political and issue advertising on their services and to clearly indicate in their advertising policies the extent to which such advertising is permitted or prohibited on their services. Thirdly, Relevant Signatories commit to make political or issue ads clearly labelled and distinguishable as paid-for content. Fourthly, Relevant Signatories commit to put in place proportionate and appropriate identity verification systems for sponsors and providers of advertising services acting on behalf of sponsors placing political or issue ads. Moreover, Relevant Signatories will make sure that labelling and user-facing transparency requirements are met before allowing placement of ads. Fifthly, Relevant Signatories commit to provide transparency information to users about the political or issue ads they see on their service. Sixthly, Relevant Signatories commit to provide users with clear, comprehensible, comprehensive information about why they are seeing a certain political or issue-based advertisement. Seventhly, Relevant Signatories commit to maintain repositories of political or issue advertising and ensure their currentness, completeness, usability and quality, along with the necessary information to comply with their legal obligations and with transparency commitments under the Code. Eighthly, Relevant Signatories commit to provide application programming interfaces (APIs) or other interfaces enabling users and researchers to perform customised searches within their ad repositories of political or issue advertising. Ninthly, Relevant Signatories commit to increase oversight of political and issue advertising and constructively assist, as appropriate, in the creation, implementation and improvement of political or issue advertising policies and practices. Tenthly, Relevant Signatories agree to engage in ongoing monitoring and research to understand and respond to risks related to disinformation in political and issued-based advertising (European Union 2022b).

In order to limit impermissible manipulative behaviour and improve the integrity of their services, Relevant Signatories commit to put in place or further bolster policies to address both misinformation and disinformation across their services, and to agree on a cross-service understanding of impermissible manipulative behaviours, actors and practices, in order to ensure a consistent approach across services. In this context, the behaviours and practices refer to, the creation and use of fake accounts, account takeovers and bot-driven amplifications; hack-and-leak operations; impersonation; malicious deep fakes; the purchase of fake accounts; non-transparent paid messages or promotion by influencers; the creation and use of accounts that participate in coordinated inauthentic behaviour; and user conduct aimed at artificially amplifying the reach or perceived public support for disinformation. This commitment to a shared understanding of impermissible manipulative behaviour is a novelty in relation to the Code of 2018 and the strengthened Code also highlights the need to continuously review and update this list of impermissible behaviours, considering the continuous evolution of disinformation dynamics (European Union 2022b).

Moreover, another novel commitment related to the integrity of the services refers to AI (artificial intelligence) systems. Relevant Signatories that develop or operate AI systems commit to take into consideration the transparency obligations and the list of manipulative practices prohibited under the proposal for Artificial Intelligence Act (European Union 2022b).

Furthermore, Relevant Signatories commit to operate channels of exchange between their relevant teams in order to proactively share information about cross-platform influence operations, foreign interference in the information space and relevant incidents that emerge in their respective services, aiming at preventing the dissemination and resurgence of disinformation, in full compliance with privacy legislation and due consideration for security and human rights risks (European Union 2022b).

The European Commission recognises that the users are to some extent part of the problem associated with the dissemination of disinformation and thus also part of the solution. The COVID-19 crisis highlighted that the viral spread of information with no malicious intention – misinformation – by users may have serious implications, consequently demanding the creation of initiatives and commitments to empower users. Accordingly, the European Commission understands that by providing users a better understanding of the functioning of online services, as well as tools that foster more responsible behaviour online and that enable users to detect and report false and/or misleading content can dramatically limit the spread of disinformation. Therefore, Relevant Signatories commit to continue and enhancing their efforts in media literacy and critical thinking (European Union 2022b).

Furthermore, as a novelty in relation to 2018, the European Commission highlights that the design and the architecture of online services have a significant impact on the behaviour of users online. Consequently, requiring the assessment of the risks underlying online systems and the design of architectures to minimise those risks particularly linked to the spread and amplification of disinformation. Accordingly, Relevant Signatories commit to minimise the risks of viral propagation of disinformation by adopting safe design practices as they develop their systems, policies and features. Moreover, recommender systems have a significant impact on what information is actually accessed by users. Thus, the European Commission understands that there is a need to improve the visibility of reliable information and, at the same time, these systems should be transparent in terms of the criteria used for prioritising or de-prioritising content, and should be design to minimise the risks associated with the viral spread of disinformation. Therefore, Relevant Signatories commit to make recommender systems transparent to the recipients regarding the main criteria and parameters used for prioritising or de-prioritising content and to provide options to users about recommender systems, and to make available information on those options. Additionally, Relevant Signatories also commit to empower users with tools to assess the provenance and edit history, authenticity, or accuracy of digital content (European Union 2022b; European Commission 2021b).

In addition, the strengthened Code also commits to equip users to identify disinformation. Therefore, aiming to enabling users to navigate in their services in an informed way, Relevant Signatories commit to strengthen their efforts to better equip users to identify disinformation. Moreover, Relevant Signatories commit to facilitate, across all member states languages in which their services are provided, users access to tools for assessing the factual accuracy of sources through fact-checks from fact-checking organisations that have flagged potential disinformation, as well as warning labels from other authoritative sources. The Code does not aim to evaluate the veracity of editorial content, however the abundance of information available online challenges users in terms of which information sources to consult and trust. Hence, Relevant Signatories commit to provide users with tools to empower them to make more informed decisions when they encounter online information that may be false or misleading, and to facilitate user access to tools and information to assess the trustworthiness of information sources (European Union 2022b; European Commission 2021b).

As previously mentioned, the European Commission recognises the fundamental role of users as part of the solution, therefore the strengthened Code aims to commit Relevant Signatories to create a user-friendly and effective functionality that enables users to flag disinformation with the potential to cause public harm or individual harm. Hence, Relevant Signatories commit to provide users with the functionality to flag harmful false and/or misleading information that violates Signatories policies or terms of service (European Union 2022b; European Commission 2021b).

Additionally, another novelty of the strengthened Code in relation to 2018 is the commitment to an appropriate and transparent mechanism that explains the reasons of why an account or content have been flagged as disinformation and also the commitment to provide access to those who have been flagged to seek redress against the measures applied. Therefore, Relevant Signatories commit to create a transparent appeal mechanism to inform users whose content or accounts have been subject to enforcement actions and provide them with the possibility to appeal against the enforcement action at issue and to handle complaints in a timely, diligent, transparent and objective manner and to reverse the action without undue delay where the complaint is deemed to be founded (European Union 2022b; European Commission 2021b).

Furthermore, considering the broaden participation to include messaging services, the strengthened Code also commits to measures to curb disinformation on messaging apps to help users to verify whether a particular content they received has been fact-checked as false and to identify disinformation, in full compliance with the nature of these services and in particular regarding the right of private communications and without weakening encryption. Therefore, Relevant Signatories commit to continue to build and implement features or initiatives that empower users to think critically about the information they receive and to help them to determine whether it is accurate, without any weakening of encryption and with due regard to the protection of privacy (European Union 2022b; European Commission 2021b).

The European Commission recognises that the research community is fundamental to understand the evolution underlying the risks and challenges related to disinformation, because they offer evidence-based analysis and thus have a fundamental role in supporting the creation of risk mitigation mechanisms. The access to online platforms data is essential for research activities. Therefore, the strengthened Code aims to set up a framework for robust access to platform data by the research community and adequate support for their activities as part of an effective strategy to tackle disinformation. At the same time, the European Commission clearly highlights that the conditions for access to data for research purposes, should be transparent, open and non-discriminatory, proportionate and justified. In addition, as far as it concerns personal and sensitive data, the conditions must be fully compliant with the General Data Protection Regulation (GDPR) and should respect the rights and legitimate interests of all concerned parties. Hence, Relevant Signatories commit to provide access, wherever safe and practicable, to continuous, real-time or near real-time, searchable stable access to non-personal data and anonymised, aggregated, or manifestly-made public data for research purposes on disinformation through automated means. Moreover, in terms of access to data requiring additional scrutiny[62], Relevant Signatories commit to provide vetted researchers with access to data necessary to undertake research on disinformation by developing, funding, and cooperating with an independent, third-party body that can vet researchers and research proposals.

[62] Data requiring additional scrutiny refers to data that requires additional scrutiny and safeguards, which might expose personal information, including sensitive information, confidential information, such as trade secrets, or data linked to the security of the platforms.

Furthermore, Relevant Signatories commit to support good faith research into disinformation that involves their services (European Union 2022b; European Commission 2021b).

Additionally, other stakeholders involved in research activities about disinformation such as civil society organisations, non-academic research centres and investigative journalists also play important roles in the detection and analysis of disinformation campaigns, the formulation of policy responses, as well as on the promotion of public awareness and social resilience. Therefore, there is a need to allow, in particular in member states where is not adequate academic capacity, a sufficient level of access to data to those stakeholders, in full compliance with privacy requirements and subject to reinforced control against misuses of personal data. Thus, Relevant Signatories commit to conduct research based on transparency methodology and ethical standards, as well as to share datasets, research findings and methodologies with relevant audiences (European Union 2022b; European Commission 2021b).

The European Commission recognises the fundamental role of the fact-checking community in assessing and verifying content, based on facts, evidence and contextual information, and also on raising awareness about online disinformation. Therefore, the strengthened Code introduces commitments to provide access to platform data by the fact-checking community and commitments to adequate support for their activities, as part of an effective strategy for tackling disinformation, in full compliance with the right to private communications and appropriate protection of the rights and legitimate interests of all concerned parties. Moreover, the Code also highlights the need for online platforms to extend their cooperation with fact-checkers to ensure the consistent application of fact-checking in their services, with a particular focus on member states and languages where fact-checking is not yet provided. Yet, fact-checking organisations need to be verifiably independent from partisan institutions and transparent in their finances, organisation and methodology. Therefore, Relevant Signatories commit to establish a framework for transparent, structured, open, financially sustainable, and non-discriminatory cooperation between them and the EU fact-checking community regarding resources and support made available to fact-checkers. Moreover, Relevant Signatories also commit to integrate, showcase, or otherwise consistently use fact-checkers' work in their platforms' services, processes and contents, with full coverage of all member states and languages. Furthermore, one the one hand, Relevant Signatories commit to provide fact-checkers with prompt, and whenever possible, automated access to information that is pertinent to help them maximise the quality and impact of fact-checking activities. On the other hand, fact-checking organisations commit to operate on the basis of strict ethical and transparency rules, and to protect their independence (European Union 2022b; European Commission 2021b).

Despite the innovation underlying the Code of Practice in terms of the efforts to tackle disinformation, the Report Assessment 2020 highlighted the limit quality of reporting and the absence of an independent assessment. The reporting and the monitoring processes are fundamental to regularly assess the implementation of the commitments by the Signatories and to evaluate the effectiveness of the Code as a central piece to tackle disinformation. Accordingly, to support the monitoring process a Transparency Centre and a Permanent Task-force were created (European Union 2022b; European Commission 2021b).

The Transparency Centre is a publicly available website that contains all the information related to the implementation of the Code, easy-to-understand, *per* service, easily searchable and that is updated in a timely and complete manner, aiming to enhance the transparency and accountability underlying the implementation of the Code. Moreover, to support the monitoring process, a Permanent Task Force was created to provide input in view of technological, societal, market, and legislative developments relevant for the review and adaptation of the Code, and includes the Signatories, the European Commission, the European External Action Service, the European Regulators Group for Audiovisual Media Services (ERGA), the European Digital Media Observatory and other invited-third parties independence (European Union 2022b; European Commission 2021b).

Nevertheless, despite the relevance of the monitoring process, the voluntary and self-regulation nature of the Code potentially limits the successful accountability of the Signatories and the effectiveness of the Code as a tool to tackle disinformation. In this context, the European Commission proposed in December 2020 a regulation piece, the Digital Service Act, that was agreed between the European Parliament and Member States in April 2022 and aims to ensure a safer and accountable online environment. However, the Act is more focused on illegal content rather than disinformation. In terms of disinformation, is very subtle and limited to transparency measures, such as obligations with transparency reporting; requirements on terms of service in full compliance with fundamental rights; user-facing transparency of online advertising; user choice not to have recommendations based on profiling; codes of conduct; and ban of a certain type of targeted advertising on online platforms containing political views[63].

[63] For a deeper understanding of this initiative see https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

Therefore, to sum up, despite the innovation underlying the Code of Practice, the COVID-19 pandemic crisis highlighted the limitations and shortcomings underlying the effectiveness of the Code to tackle the proliferation of disinformation, particularly in terms of the inconsistent and incomplete implementation of the Code. Consequently, a strengthened Code entered into force with more players involved, smaller and specialised platforms, the online advertising industry, ad-tech companies and fact-checkers. Moreover, the Code was adapted to include new manipulative behaviour, such as fake accounts, bot-driven amplification, impersonation and deep fakes. Furthermore, the European Commission acknowledged the fundamental role of users as an active part of the response to online disinformation. Hence, introducing commitments to flag disinformation, but also to enhance media literacy, foster access to reliable information and ensure the safe and transparent design of the architecture and recommender systems of online platforms, as well as the creation of mechanisms to appeal in case of accounts and/or content being flagged as disinformation. Nevertheless, despite these positive initiatives, the voluntary and self-regulation nature of the Code, the absence of a structured independent assessment and the lack of sanctions in case of non-compliance with the commitments hold the potential to contribute to a limited effectiveness of the Code. Yet, the Digital Service Act may be the starting point to create a framework to co-regulate of online platforms and improve the effectiveness of the Code as a tool to tackle disinformation.

In conclusion, the security governance of online disinformation at EU level is based on a strategy of democratic deterrence that privileges measures to improve the democratic resilience of the European society rather that criminalising or prohibiting the spread of disinformation. This strategy results from the understanding of the European Union concerning the main factors that contribute to the spread and resilience of disinformation. Accordingly, the EU recognises the role that citizens play in unintentionally share false and/or misleading content, which in combination with the current political and economic context makes the spread of disinformation more successful. Hence, measures to raise awareness, enhance media literacy and to improve the resilience of European democratic societies are at centre of the action of the EU against disinformation. Moreover, the Union acknowledges the positive role of online platforms in terms of democratising the access to information, but it also recognises their use to create, disseminate and amplify disinformation. Therefore, the European Commission created an innovative tool, the Code of Practice, to commit Relevant Signatories involved in the online ecosystem to certain actions and initiatives that aim to create a safer, transparent and accountable ecosystem. Overall, the strategy of the EU against disinformation confirms the preoccupation to adopt a proportional level of reaction that do not exceed what is necessary to achieve the objectives. The EU constantly demonstrates in its discourse the preoccupation with the protection of fundamental rights and freedoms, in particular freedom of expression, and also throughout the initiatives created, that are focused on protecting freedom of expression rather than banning disinformation. Nevertheless, the COVID-19 crisis demonstrated the limitations of this response, particular in terms of the implementation of the Code of Practice, with implications for the effectiveness of the strategy of the European Union to tackle disinformation, and ultimately to the protecting of the freedom of expression itself, which will be further discussed in the next chapter.

CHAPTER 6

Denying, Punishing or neither? the inconsistencies and limitations underlying the security governance of online disinformation at EU level

The objective of this chapter is to analyse the *structures*, the main initiatives and the actors, involved in the security governance of online disinformation at EU level through democratic deterrence, in terms of measures of punishment. Moreover, this chapter also uses the model proposed by Hellman and Wagnsson (2017) to identify the inconsistencies and limitations of the security governance of online disinformation at EU level in order to clarify how the response of the European Union to disinformation relates to proportionality and effectiveness and its implications to overcome the dilemma of effectively respond to disinformation without jeopardizing fundamental rights and freedoms.

As previously mentioned in chapter one, this study does not aim to evaluate the effectiveness of the response of the European Union to online disinformation. Nevertheless, we understand that there is a need to pay closer attention to the design of the response, namely in terms of its inconsistencies and limitations, because, as already noticed, there is proportionality in the action of the EU to disinformation. Yet, if the rigid concern with proportionality has the potential to limit effectiveness of the actions against online disinformation, fundamental rights and freedoms such as freedom of expression remain at risk. The EU understands freedom of expression beyond freedom to express, but also freedom from being manipulated. Accordingly, although the level of reaction to online disinformation at EU level demonstrates proportionality, and at first hand does not create further insecurities related to the violation of fundamental freedoms and rights, the limited effectiveness of the response may potentially be exploited by adversaries, as the COVID-19 pandemic crisis demonstrated, allowing the spread of disinformation and hence freedom of expression remains at risk. Consequently, with implications for the successful overcoming of the dilemma of responding effectively to disinformation without jeopardizing fundamental rights and freedoms, considering that is just partially achieved because the effective response remains short of action.

Therefore, this chapter contributes to the analysis concerning the principle of proportionality in the security governance of online disinformation at EU level through measures of punishment and its implications on the overall security governance of online disinformation, and answers the following questions: *What punishment initiatives have been defined by the European Union to respond to disinformation as a threat to the foreign policy objectives in the eastern neighbourhood and as a hybrid threat to the European democratic, economic and social project? Which actors are involved in these structures? Which type of action – confronting, blocking, naturalising or ignoring – better describes the strategy underlying the security governance of online disinformation at EU level? How does the security governance of online disinformation at EU level considers proportionality?*

6.1. Deterring Online Disinformation through punishment

The European Union recognises that despite the fundamental role of the initiatives to improve democratic resilience in response to online disinformation they are not sufficient, and thus, are accompanied by a strategy of punishment through compellence. Compellence is a strategy that aims to challenge the strategic calculus of the aggressor, traditionally through military posturing or coercive diplomacy. However, Wigell (2021) considers that democracy itself can also be used as a form of compellence in response to authoritarian systems, considering its potential to challenge authoritarian control (p.60).

The strategy of punishment at EU level is mostly operationalised through actions to detect, analyse and expose disinformation. At the same time, the European Union recognises, since the creation of the response to disinformation, the need to improve its strategic communication through the Strategic Communication Task Forces of the European External Action Service, further discussed in chapter five. Accordingly, by exposing disinformation campaigns, the European Union aims to impact the strategic calculus of the aggressor and challenge the effectiveness of these campaigns, because citizens are more aware of its existence. To support these actions, the European Commission and the High Representative highlight the fundamental role of the Strategic Communication Task Forces of the European External Action Service, but they also consider that it is necessary to reinforce the Union Delegations and the EU Hybrid Fusion Cell with additional specialised staff, such as experts in data mining and analysis to process the relevant data, and new tools. In addition, the Commission and the High Representative also recognise that threat analyses and intelligence assessments are fundamental to detect and expose disinformation, thus the expertise of the Intelligence and Situation Centre should be fully used (European Commission and High Representative 2018a).

Security agencies, through for instance intelligence, are better prepare to collect information about the source and support a more effective response. However, these security organisms have a complicated relation with democracy, because they tend to be under weak democratic control and can contribute to excessive influence in the democratic process (Tenove 2020 p.524).

Moreover, despite its relevance, debunking disinformation has some limitations, particularly when fact-based information used to confront disinformation campaigns is more complex, which makes it less understandable and ineffective than simple false or misleading information already widespread in the information space (Baer-Bader 2020, p.2). In addition, Helm and Nasu (2021) argue that "psychological biases have been shown to make people resistant to information correction, particularly where fake news is consistent with their beliefs or cultural outlook" (p.326). Furthermore, political disinformation tends to be highly emotional and even more challenging to counter (Baer-Bader 2020, p.2).

In the context of the European Union, the COVID-19 pandemic crisis demonstrated the limitations underlying debunking and the ineffective strategic communication at EU level. Despite the aid scheme worth it up to 200€ billion provided by the European Union to Italy, the absence of a coherent policy, the slow response in the early stages of the pandemic and the social anxieties associated with the crisis created fertile ground for disinformation to proliferate easily in Italy. This situation was accompanied by an ineffective response to disinformation at EU level, focused on debunking disinformation and with limited action in terms of strategically communicating the actions of the Union in response to the pandemic crisis. Consequently, the absence of a coherent policy to aid Italy, the lack of a clear and effective strategic communication at EU level in terms of promoting the policies and the actions taken to respond to the pandemic crisis, were successfully exploited by countries such as Russia and China. Russia filled this gap with an intensive propaganda campaign of sending immediate military medical aid convoys, with implications for the perception of the majority of people in Italy which saw the European Union as part of the problem rather than the solution (Baer-Bader 2020; Pamment 2020; Vériter, Bjola and Koops 2020).

Therefore, identifying and exposing disinformation campaigns is important, but if not accompanied with a clear and effective strategic communication action it is potentially ineffective to contain the spread disinformation, and event to have harmful backfire effects (Helm and Nasu 2021, p.326). Hence, there is an urgent need for the European Union to improve its strategic communications in general and in times of crisis in particular, and engage in a more proactive and robust response that gives visibility to EU action and that actively promotes its policies, actions and success that has achieved so far (Baer-Bader 2020, pp.2-3).

Furthermore, the European Union also uses in terms of punishment actions, in its external action, in particular in the eastern neighbourhood, democratic compellence and more recently sanctions on the media against Russia.

The development and implementation of programs that promote democracy and human rights in the neighbourhood of authoritarian states can be used as democratic compellence. Accordingly, cultivating democratic principles and values through networks and proxies by means of soft power and public diplomacy threaten authoritarian states, because of the potential emergence of bottom-up democratising movements. The support to social and political activism by western liberal democracies creates a tricky choice for authoritarian regimes, between allowing those relations, risking deepen citizen activism or harden the pressure on civil society and further eroding legitimacy. Hence, signalling preparedness and will to support democracy, human rights and civil activism is a form to threaten autocracies. However, this type of action can be interpreted and exposed as an alternative form of interference and influence (Wigell 2021, pp.62-63). Nevertheless, Wigell (2021) considers that hybrid interference is different from the promotion of democracy and human rights. Whereas hybrid interference and influence are forms of covert manipulative interference, the promotion of democracy tends to be open, overt and transparent and thus considered a form of legitimate public diplomacy in compliance with international law. Yet, despite its legitimate action, the impact and effects underlying the promotion of democracy and human rights should not be overstated. The response from authoritarian regimes to any dissent is likely to happen, but it also has the potential to reinforce the action of democracies on exposing authoritarianism and favour the objectives of democracies and boost their soft power (p.63).

At the EU level, this type of action occurs mostly in the response to disinformation as a threat to the foreign objectives in the eastern neighbourhood. In this context, the European Union, through the Action Plan on Strategic Communication presented by the High Representative in 2015, highlighted the relevance of engaging with civil society and recognised the role of civil society as integral part of the response to disinformation. On the one hand, measures to increase public awareness for the existence of this type of campaigns are privileged. On the other hand, civil society and citizens are supported to work as a "media watch dog" and to hold governments to account, through activities that promote the development of critical thinking and media literacy (High Representative 2015).

In terms of the sanctions against Russia in the form of restrictions on the media, the European Union, in response to the illegal annexation of Crimea in 2014, Russia's unprecedented and unprovoked military attack against Ukraine in 2022 and the illegal annexation of Donetsk, Luhansk, Zaporizhzhia and Kherson in 2022, has decided to approve a package of sanctions and restrictive measures against Russia over Ukraine, aiming to significantly curtailing is ability to wage war. In this context, we highlight in particular, for the purposes of this research, the restrictions imposed by the European Union on the media. The European Union acknowledges that Russian media have been used by the Russian government to manipulate information and promote disinformation about the invasion of Ukraine, including disinformation to also destabilise the neighbouring countries and the European Union and its member states. Therefore, in March and June 2022 the European Union has suspended the broadcasting activities of five Russian state-owned outlets (Sputnik, Russia Today, Rossiya RTR/RTR Planeta, Rossiya 24/Russia 24, TV Centre International). Moreover, in this context, the European Union reinforced its commitment to firmly respond to foreign information manipulation and interference in whatever shape or form[64].

In conclusion, as far as it concerns the security governance of online disinformation at EU level in terms of the democratic deterrence through punishment, the European Union uses actions to detect, analyse and expose disinformation and also strategic communications. However, these actions have proven so far rather limited in terms of debunking and ineffective in terms of strategic communication. At the same time, the European Union, in its external action, has been using democratic compellence and more recently sanctions in the form of restrictions on the media against Russia. Yet, this last measure is somewhat inconsistent with the overall strategy of the European Union to disinformation. Until this moment the EU has always discursively focused on highlighting that its response to disinformation was based on protecting freedom of expression rather than prohibiting disinformation. So, it would be of added value for the European Union to clarify what kind of behaviour in the information space is impermissible and that will be met with more assertive measures and adapt its overall strategy to this understanding.

[64] For a broader and deeper understanding about the sanctions and the restrictive measures applied by the European Union against Russia over Ukraine since 2014 see, for instance, https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/.

6.2. Confronting, blocking, naturalising and/or ignoring? the limitations and inconsistencies underlying the security governance of online disinformation at EU level

The European Union considers online disinformation as a threat and responds to it through a strategy of democratic deterrence that involves mostly measures of denial aiming to improve democratic resilience, but also measures of punishment. At the same time, the EU acknowledges the need to respond effectively to online disinformation without jeopardizing fundamental values and freedoms, in particular freedom of expression. Yet, although the European Union normatively justifies its action against disinformation and constantly demonstrates preoccupation with proportionality, both discursively and in terms of the actions implemented to respond, the security governance of online disinformation at EU level has some limitations and inconsistencies, that may potentially be exploited by adversaries and further weakening and undermining the response to online disinformation (Pamment 2020, p.5). Consequently, this may have implications in terms of the dilemma underlying the response, because despite the proportionality in the reaction, the limitations in terms of effectiveness means that part of the dilemma is not overcome and the spread of disinformation continues, with implications for the protection of freedom of expression itself. Therefore, to clarify the identification of these limitations and inconsistencies of the overall strategy of the European Union to tackle online disinformation we use the model proposed by Hellman and Wagnsson (2017).

This model proposes four types of actions to respond to disinformation – confronting, blocking, naturalising and ignoring. Confronting and blocking offer a more engaging response and offensive posture that actively confronts or blocks the perceived external adversarial narratives. Whereas naturalising and ignoring offers a less engaging response and a more defensive posture based on the projection and protection of a narrative that promotes one's model instead of confronting or blocking a particular adversarial narrative (Hellman and Wagnsson 2017).

In the European Union, initially, the objectives underlying the response to online disinformation, introduced in the Action Plan on Strategic Communication presented by the High Representative in 2015, aimed mostly to improve the strategic communication of the EU in the eastern neighbourhood, by producing and projecting a positive and appealing narrative of the EU to the neighbourhood. Moreover, the European Union aimed to protect its narrative in the region, by strengthening the media environment and increasing public awareness of disinformation activities by external actors. Therefore, the initial strategy was based on naturalising actions focused on projecting a positive narrative of the policies and values of the EU in the region to win the trust of the audience. At the same time, an ignoring strategy was also implemented, assuming that democracy is not only a vulnerability, but also an asset used to defend and protect an honest, open and fair society, namely by actively reinforcing and improving the resilience of the civil society.

In terms of the actions underlying the naturalising strategy that aimed to promote an effective communication of its policies and values in the eastern neighbourhood, the EU introduced measures to increase its strategic communication capacity, namely through the creation of the East StratCom Task Force in the European External Action Service. In addition, the EU recognised the need to create networks at EU level, between EU institutions, delegations and member states to improve the coordination and coherence of European messaging to the eastern neighbourhood. Furthermore, the EU also uses its EU funded programs, projects and activities in the eastern neighbourhood to improve the effectiveness of its communication activities. The EU understands that it needs to be closer to local populations and implement public diplomacy initiatives that involves the engagement with local populations, namely the youth, academia and civil society to effectively explain its policies, promote dialogue and ensure that citizens are informed properly about the EU. Moreover, the EU also aims to support pluralism and its strategic communication in the Russian language and provide information in local languages from different sources other than Russian.

Furthermore, in terms of the actions underlying the ignoring strategy, the EU defined and implemented actions to engage with local populations, namely the youth, academia and civil society to increase awareness, develop critical thinking and promote media literacy, in order to train citizens to critically assess information and improve societal resilience in the region. At the same time, the Union aims to strengthen the media environment in the region by creating networks that should include and involve journalists and media representatives; by supporting independent media and freedom of the media and of expression; and by supporting the capacity building for journalists and media actors and improve quality media and journalism as fundamental to defend, protect an honest, open, fair and informed society.

Nevertheless, although the strategy of the European Union in terms of responding to disinformation in the eastern neighbourhood is mostly based on a defensive posture, the EU also engages in a more offensive behaviour through confronting actions, namely by exposing disinformation campaigns in the region and by producing counter-narratives that refute or reinterpret particular events. In this context, according to Wagnsson and Hellman (2018, p.1162), the activities related to the identification, analysis and report of disinformation trends, namely through Disinformation Digest[65], can be considered has highly controversial and may contradict the uniqueness of the European Union as an international actor, particularly how it depicts external actors. Disinformation Digest has been representing Russia as the 'other' and antagonically, "as inferior, as a threat, and as a violator of universal norms" (Wagnsson and Hellman 2018, p.1170). A normative power "should communicate in a non-antagonistic, humble way and avoid constructing others in ways that sustain hierarchies that can stir conflict" (Wagnsson and Hellman 2018, p.1161). Therefore, by employing a confronting approach, trough Disinformation Digest, the EU uses an 'othering' strategy, that creates an antagonistic division between 'us' and the 'other', which can contradict its normative power and prompt conflict situations. Furthermore, this type of strategy has also some limitations related to psychological bias.

Today, the main objective of the European Union in responding against disinformation is the protection of the European project at all levels. The EU understands that disinformation is a complex and evolving challenge, with multiple origins, forms and implications and demands a calibrated response to avoid a symmetrical action. Therefore, the response of the European Union to online disinformation aims to improve the capabilities of Union institutions to detect, analyse and expose disinformation. Second, the EU aims to strengthen coordinated and joint responses to disinformation. Third, the EU aims to mobilise the private sector to tackle disinformation. Fourth, the EU aims to raise awareness and improve societal resilience (European Commission and High Representative 2018a). To this end, the strategy of the European to tackle disinformation is based on democratic deterrence and involves a mix of a defensive posture, through measures of denial and an offensive posture, through measures of punishment.

In terms of the defensive measures, the European Union considers democracy beyond a vulnerability, as the most important tool to tackle disinformation, because of its capacity to improve societal resilience and deny the success of interference and manipulation. Therefore, the EU implements actions that follow an ignoring strategy focused on raising awareness to improve societal resilience, on strengthening the coordination and joint responses to

[65] Disinformation Digest is a review that exposes disinformation narratives based on the results of selective media monitoring.

disinformation, and also on mobilising the private sector to build a more transparent, trustworthy and accountable online ecosystem.

However, the mobilisation of the private sector and in particular the implementation of the Code of Practice has some limitations, in particular related to the accountability of the Signatories and the effectiveness of this tool to tackle online disinformation. In this context, the European Union considers that regulating online platforms is best done through voluntary-based measures, because the private sector has the expertise and the instruments needed to address the vulnerabilities that allow the proliferation of disinformation. Yet, this assumption holds limitations and is potentially problematic, mostly because it heavily depends on the commitment and good will of the online platforms to respond to disinformation, which is challenged mostly by the economic model of these platforms. Accordingly, the economic model of online platforms is based on the engagement of its users and the viral proliferation of disinformation keep users engaged. Therefore, there is a contradiction between the necessity to keep users engaged for profit and the interest of democratic governments and international organisations to safeguard the integrity of the democratic process while ensuring freedom of expression (Durach, Bârgăoanu and Nastasiu 2020, pp.14-15). Furthermore, online platforms argue that they, conveniently, prefer to respond to suspicious behaviour and reduce the visibility of disinformation content, rather than eliminating this content outright. Additionally, the monitoring process foreseen in the Code of Practice is limited to provide information concerning the measures that platforms are implementing and the effectiveness of those measures remains a dark area (Saurwein and Spencer-Smith 2020, pp.834, 836). Moreover, self-regulation also has other challenges associated with the enormous amount of content to monitor, the limited efficiency of fact-checking activities as already mentioned, and the normal failures of human moderation. Furthermore, the option of this approach highlights the difficulty to establish regulations for a domain lacking transparency and accountability particular in terms of this type of content (Durach, Bârgăoanu and Nastasiu 2020, pp.14-15).

The European Union considers that the security governance of online disinformation should be fundamentally based on a defensive posture, through protecting freedom of expression rather than criminalising or prohibiting online disinformation, nevertheless, at the same time, the EU recognises that is not sufficient. Therefore, the European Union also engages in a more offensive posture through confronting actions to improve the capabilities of Union institutions to detect, analyse and expose disinformation and strategic communication that aim to refute and reinterpret particular events with empirical evidence and trustworthy sources to challenge the success and the strategic calculus of the aggressor. However, the COVID-19 pandemic crisis demonstrated that the impact of these actions to tackle the spread of disinformation has proved to be rather limited. Debunking disinformation although important, if not accompanied by a clear and effective strategy of strategic communications that gives visibility to the success and actions of the European Union risks being exploited by adversaries with implications for the overall strategy of tackling disinformation.

Moreover, in terms of punishment actions the European Union also engages in a naturalising strategy by promoting positive messages of EU policies and democratic values in the eastern neighbourhood.

In addition, more recently, in the context of Russian invasion of Ukraine the EU also engaged in a blocking strategy by suspending the broadcasting activities of five Russian state-owned outlets. This demonstrates inconsistency, because the European Union highlights constantly that its responses is based on the protection of freedom of expression rather than prohibiting disinformation, this can be exploited by adversaries as an example of democracies violating democratic values.

Furthermore, another challenge underlying the response to disinformation is the multi-dimensional approach to disinformation. Although the complexity underlying online disinformation demands a multi-dimensional governance it has implications and challenges for the accountability of every party involved. Accordingly, Saurwein and Spencer-Smith (2020) argue that "a multi-dimensioned approach to disinformation should also clearly allocate accountability in a shared, distributed and cooperative structure. [because] this variety risks confusion around accountability and shirking of responsibility" (p.836).

In conclusion, the strategy of democratic deterrence employed by the European Union against disinformation is mostly based in ignoring actions. Whereas improving societal resilience through critical thinking and media literacy, strengthening quality journalism and the electoral process, and increasing the transparency and responsibility of online platforms are crucial to tackle the spread of disinformation. The limitations and inconsistencies underlying the actions of the European Union in response to disinformation risks being exploited by adversaries, demanding the development of more pre-emptive and accountability mechanisms. In particular, in terms of a new regulatory regime of online platforms and a strong policy of strategic communications (Durach, Bârgăoanu and Nastasiu 2020; Pamment 2020; Vériter, Bjola and Koops 2020).

Conclusions
The consideration of proportionality in the security governance of online disinformation at EU level

This study analysed the strategy of the European Union to tackle online disinformation to evaluate the consideration of the principle of proportionality in the equation of the response and we argue that there is proportionality in the security governance of online disinformation at the EU level. The European Union is able to justify its moral ground to act and there is a widespread concern in responding with proportional measures that consider the nature of the harm and that are focused on protecting the realisation of fundamental rights and freedoms in the response. The European Union continuously highlights that the response to online disinformation is focused on protecting freedom of expression rather than criminalising or prohibiting this type of content. Nevertheless, the security governance of online disinformation at EU level has multiple limitations and inconsistencies with implications for the effectiveness of the action against this challenge. Consequently, despite the concern of the European Union with the dilemma of responding effectively to online disinformation without jeopardizing democratic values and principles, the limited effectiveness has been exploited by adversaries as the COVID-19 pandemic crisis demonstrated, thus the dilemma is partially addressed and the balance between effectiveness and proportionality is at crossroads.

Disinformation is not a new phenomenon neither in domestic nor in international politics, yet the current political, economic and mostly the technological context contributed to an easier and more effective use of this type of content. Consequently, online disinformation has come to be understood as a security threat at the political and at the academic levels and responding to it has been considered to be often appropriate by democracies, particularly because of its potential to undermine democratic life (Tenove 2020, p.524). At the same time, democracies have an asymmetric disadvantage, because they are an easy target and a fragile responder, because the strategies implemented can generate other insecurities and represent a shift in the posture of democracies in the international system (Paterson and Hanley 2020, p.442). Therefore, addressing online disinformation has been accompanied by a dilemma of defining and implementing an effective response without jeopardizing democratic values and fundamental rights and freedoms.

In the European Union, the preoccupation with the phenomenon of disinformation is not new. The virtual and the physical distance between the European Union and its citizens has been exploited by multiple actors to misinform on issues about the Union (Hedling 2021). Nevertheless, this preoccupation was met with limited action, in particular through the reform of the European governance in 2001 that aimed to bring the European Union closer to its citizens.

Only in 2015, the European Union considered disinformation as a threat. However, the understanding of this phenomenon in security terms as been evolving in terms of its conceptualisation and reaction.

In 2015, in response to the use of communication tools by Russia in the eastern neighbourhood, mostly in the form of disinformation, the European Union manifested a more assertive posture in relation to disinformation as a threat. Accordingly, the European Council of March 2015 stressed the "need to challenge Russia's ongoing disinformation", because disinformation was considered an external threat with origins in Russia to the realisation of the foreign policy objectives in the eastern neighbourhood.

In order to understand how does the use of disinformation by Russia in the eastern neighbourhood affects the realisation of the foreign policy objectives of the European Union in the eastern neighbourhood we considered the triangular interaction between the European Union, Russia and the neighbouring state, in this case Ukraine.

In terms of the interaction between the European Union and Ukraine, we considered the European Neighbourhood Policy (ENP) and the Eastern Partnership (EaP) that institutionalises the relations between these two actors. The creation of these foreign policy instruments was based on the assumption that the neighbourhood is simultaneously an opportunity and a challenge. On the one hand, the European Council of December 2002, that inaugurated the discussion for the creation of the ENP, considered the enlargement of the EU as an opportunity to deepen relations with the neighbours and project the European project. At the same time, on the other hand, it also recognised that the enlargement brought the Union closer to instability. Consequently, in the Communication on "Wider Europe – Neighbourhood: A New Framework for Relations with our Eastern and Southern Neighbours" (2003) the European Commission recognised the potential impact of an event occurring outside the EU to the Union itself. Accordingly, the peace, security and prosperity of the EU begins beyond its borders. This assumption is reinforced in the European Security Strategy of 2003. Hence, the European Union created the European Neighbourhood Policy and the Eastern Partnership to prevent the creation of new dividing lines between the EU and its new neighbours, and to promote political and economic reforms in the region without the prospect of membership, and thus promote peace, stability and prosperity in the region with, contributing to a greater presence and responsibility of the UE in the region (Casier 2012; Fernandes 2012; Korosteleva 2011).

This proximity between the EU and its neighbours contributed for the development of a situation of tension between the European Union and Russia. Hence, the external action of the EU in the eastern neighbourhood has been accompanied by a widespread assumption that the EU and Russia have been competing for influence in the region (Fernandes 2012). In this context, Russia has been using many strategies, including communication tools in the form of disinformation to impact the political, economic and security context of the region and challenge the influence of the EU.

Moreover, Russia has been using hybrid threats in the form of disinformation not only in the eastern neighbourhood, but also against the EU itself (Chappell, Mawdsley and Galbreath 2019). Consequently, in 2016 the European Commission and the High Representative introduce a European Union response to counter hybrid threats. In this context, the EU understands that Russia is a bigger threat in terms of the use of disinformation because is systematic and well resourced (European Commission and High Representative 2018a).

Therefore, since at least 2016, and reinforced in the Strategic Compass 2022, that the European Union understands that hybrid threats in the form of disinformation with origin in Russia does not only impact the realisation of the foreign policy objectives of the EU in the eastern neighbourhood, but also the European project itself at many levels, at the security, democratic, economic and social levels.

The European Union understands that the use of online disinformation by Russia has multiple implications for the security of the Union and for its democracy. The EU considers that this coordinated effort by Russia to interfere in the information space aims to distort the truth, to sow doubt, to gather domestic support, to challenge democratic institutions and processes, to weaken the cooperation within the EU, to divide the EU and to foment a strategic split between the EU and its North American partners. Consequently, it threatens the sovereignty of the EU and its member states, its political independence, its territorial integrity, and the security of its citizens (European Parliament 2016).

The European Union recognises that the use of disinformation is not new, but the existence of international actors and states that do not share the same interests and values of the EU and that are competing for power and using interference strategies such as disinformation are of particular concern today (European Commission 2018b). At the same time, the possible use of these strategies in the context of the European elections of 2019 and in the more than 50 presidential, national and local elections occurring in member states in 2020, triggered a more assertive posture at EU level.

The European Union considers that a healthy and resilient democratic society is based, among other things, on an informed, active and empowered society, not only at election time but all the time. The EU underlines that democratic societies depend on a meaningful participation of its citizens, which are able to form their own judgements and participate in an informed way in the public debate, fundamental to the deliberative democratic process (European Commission 2020a). Accordingly, in order to have an informed participation in the public debate and in the electoral process, the Union understands that European democratic societies depend on the ability of citizens to access a plurality of verifiable information to form their opinions on different political issues (European Commission and High Representative 2018a).

However, the EU understands that the deliberate, large-scale and systemic dissemination of disinformation challenges this assumption and pollutes the democratic process at is source (European Commission 2020a). This is related to the understanding of freedom of expression at EU level. The EU considers that freedom of expression is the respect for media freedom and pluralism, and the right of citizens to hold opinions, but is also the right of citizens to receive information free from interference. Accordingly, the realisation of freedom of expression is about media freedom and freedom to express, but is also about receiving information without interference by public authorities and regardless of frontiers (European Commission 2018a). Consequently, the European Union understands that disinformation prevents the formation of an informed opinion free from manipulation, undermining the democratic participation of its citizens, with the potential to discredit and delegitimise elections, and impacting the trust of its citizens in the integrity and fairness of the electoral process, in democratic institutions and in democracy itself. Moreover, it also supports the amplification of radical and extremists' ideas and activities (European Commission 2020a).

Democracy is a foundational and core value of the European Union, is part of the criteria to integrate the European project. Hence, the EU understands that the resilience of the Union's democratic system is part of the security of the Union. Moreover, the European Union also considers that the promotion and protection of human rights is foundation for confidence and dynamism in the European economy, society and democracy and to promote an area of freedom, security and justice. Therefore, by threatening democracy and fundamental freedoms and rights the European Union considers that disinformation threatens the European project itself (European Commission 2020b).

At the same time, the European Union also understands that responding to hybrid threats in the form of disinformation is also important to its affirmation in the area of security and defence and to demonstrate capacity to respond to new emerging threats. Accordingly, the improvement of its resilience and capabilities to respond to these threats is also part of a broader objective that aims to cultivate greater responsibility for the security of the Union, but also to support its role as a credible and reliable actor in the area of security and defence at the international level (European Council 2018).

Furthermore, the European Union also understands that online disinformation has economic implications in particular with regard to the realisation of the Digital Single Market, Digital Europe and the European Digital Sovereignty.

The 22nd March 2019 European Council recognised that a strong economy is fundamental for the prosperity and competitiveness of Europe, as well as for the realisation of its leading role on the international stage. In this context, the European Commission highlights on its communications on Shaping Europe's Digital Future and on the 2030 Digital Compass the fundamental role of the digital transition for the progress, prosperity and digital sovereignty of the EU.

The European Union recognises the multiple opportunities of digitalisation for innovation, progress, prosperity, growth, jobs creation, competitiveness and for creative and cultural diversity. However, digitalisation is also accompanied by multiple challenges, including disinformation, with implications for the security of the Digital Single Market and for the realisation of Digital Europe and European Digital Sovereignty, mostly because it challenges the trustworthiness and security of the digital space. Consequently, the European Union recognises that there is a need to take a holistic approach to the digital space and implement a strategy that considers all its elements, markets, infrastructures, connectivity and also societal and cultural aspects. This is illustrated by the inclusion of disinformation in the spectrum of cyber-security challenges in the European Cybersecurity Strategy. Accordingly, the EU understands that to "truly influence the way in which digital solutions are developed and used on a global scale, it needs to be a strong, independent and purposeful digital player in its own right. In order to achieve this, a clearer framework that promotes trustworthy, digitally enabled interactions across society, for people as well as for business is needed" (European Commission 2020c).

Therefore, the European Union understands that tackling disinformation is also fundamental to the secure and trustworthy digital transition that fosters the progress, prosperity and digital sovereignty of the EU.

Moreover, the COVID-19 pandemic crisis amplified and reinforce the potential impact of disinformation at the health, economic and social levels. The European Commission recognised that the increasing dependency on cyberspace for every day activity, as a result of measures of physical isolation to contain the pandemic, was accompanied by a potential increase in the exposure of citizens to infodemic and particularly to disinformation. The EU understands that the exploitation of these vulnerabilities by malicious and hostile actors have the potential to impact personal health, public health systems, crisis management and economic and social cohesion (European Commission 2021b).

In this context, hoaxes and misleading healthcare information can be harmful and undermine efforts to respond and contain the pandemic; conspiracy theories may be associated with illegal and criminal activities and also impact the security and dignity of ethnic or religious groups; disinformation and misinformation can be used for the sale of miracle products; disinformation can be used in combination with phishing; foreign actors can interfere the information space and deceive in relation to the response of its target to disinformation and sow confusion and distrust in public institutions. Moreover, the EU considers that divisions and uncertainties underlying the crisis also created a security vulnerability with implications for the potential increasing of more sophisticated hybrid attacks particularly in the form of disinformation (European Commission 2020c).

Hence, the COVID-19 pandemic crisis amplified and reinforced the complexity and the multiple implications underlying the threat of disinformation.

To sum up, the European Union considers online disinformation as a security threat, mostly because it threatens the survival of the European project itself at all levels, at the security, political, economic and social level, therefore justifying its moral ground to act.

We argue that the European Union justifies its discursive construction of online disinformation in security terms and the moral ground to respond to this threat. The European Union used to consider disinformation as a political issue that was addressed and managed within the framework of regular politics. The preoccupation of the EU in relation to disinformation is not new, the distance between the Union and its citizens allows for actors to exploit this vacuum with disinformation. Until today, the Union has been addressing this issue through, for instance, reforms in the European governance to bring European citizens closer to the EU in order to prevent the deceiving on EU issues. However, the European Union understands that the current deliberate, large-scale and systemic dissemination of online disinformation poses an existential threat to its democratic, economic and social system and is a challenge for the survival of the European project itself. Therefore, demanding urgent measures.

Yet, at the same time, the European Union also recognises the multiple forms that disinformation may take and the dilemma of responding to disinformation without jeopardizing democratic values and fundamental rights and freedoms, therefore demanding a calibrated and proportional response. Accordingly, the European Union uses the term disinformation to refer to different phenomena, disinformation includes disinformation in the narrow sense, misinformation, information influence operations and foreign interference in the information space (European Commission 2021b). Therefore, *Disinformation* is understood as "false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm". Public harm comprises threats to the democratic political and policy-making process, as well as to public goods such as the protection of EU citizens health, the environment or security. *Misinformation* is understood as "false or misleading content shared without harmful intent though the effects can still be harmful, e.g. when people share false information with friends and family in good faith". *Information influence operations* is understood as "coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including supressing independent information sources in combination with disinformation". *Foreign interference in the information space* "often carried out as part of a broader hybrid operation, can be understood as coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents" (European Commission 2020a).

Therefore, the European Union understands disinformation as a complex and evolving threat, that needs continues assessment and adaptation. Whereas misinformation should be met with awareness, disinformation and interference requires a more assertive and coordinated posture. Consequently, the response to disinformation demands a continuous assessment and calibration of the security logics of the EU.

Initially, the objectives underlying the security governance of online disinformation at EU level aimed to promote the strategic communication of EU namely in terms of its policies and values in the eastern neighbourhood; to strengthen the overall media environment in the region; and to increase public awareness of disinformation activities by external actors and to improve the EU capacity to respond to disinformation campaigns (High Representative 2015). Therefore, considering the external dimension of these objectives the main actors involved in the implementation of these objectives were the High Representative of the Union for Foreign

Affairs and Security Policy, the European External Action Service, and the Member States, but also journalists and media representatives, civil society and external partners.

In order to achieve these objectives, the European Union set up an East StratCom Task Force with the purpose of increasing EU strategic communication capacity and improve the effectiveness of its communication in the neighbourhood. At the same time, this organism is also responsible for improving the capacity of the Union to respond to disinformation campaigns namely by identifying, analysing and exposing disinformation campaigns. Thus, also supporting activities that aim to increase public awareness of disinformation activities in the region. Therefore, as noticed in Chapter 4 this Task Force operationalises the confronting as well as the naturalising strategy of the EU in terms of responding to disinformation. On the one hand, this organism works to improve the naturalising strategy of the EU by improving the strategic communication of the EU and producing communication products to explain its policies and values. At the same time, it works to improve the capacity of the EU to confront and respond to disinformation by refuting and reinterpreting disinformation campaigns through the presentation of empirical evidence and sources that are considered to be trustworthy (High Representative 2015).

Moreover, in terms of improving its strategic communication capacity, the EU created networks between EU institutions, delegations and member states to improve the coordination and the coherence of its strategic communication in the region. Furthermore, the EU uses public diplomacy initiatives in the eastern neighbourhood and communication activities on EU funded programs, projects and activities in the eastern neighbourhood to engage with local populations and effectively explain its policies and promote dialogue to ensure that citizens are properly informed about the EU. In this context, the EU highlights also the relevance of producing communication materials in Russian to provide information in local languages different from Russian sources (High Representative 2015).

In order to strengthen the overall media environment in the region, the EU created a network of journalists and media representatives to support independent media. In addition, the Union highlighted the need to improve cooperation between national media regulators and to cooperate with external partners, like-minded third countries and regional and international organisations to support activities that aim to promote freedom of the media and freedom of expression, as wells as to support capacity building for journalists and media actors (High Representative 2015).

Today, the European Union understands the threat of online disinformation beyond its foreign policy objectives in the eastern neighbourhood. Accordingly, the EU considers that hybrid threats in the form of disinformation with origins in Russia does not only affect the objectives of the Union in the eastern neighbourhood region, but the European Union itself.

In this context, the EU considers three main factors that contribute to the spread of online disinformation. Firstly, the EU considers that the dissemination of disinformation is both a cause and a symptom of a wider phenomenon related to the rapid change that societies are facing, economically, politically and culturally. Accordingly, there is a widespread sense of economic insecurity, rising extremism and cultural shifts that are generating anxiety and creating fertile ground for disinformation to spread and fuel societal tensions, polarisation and distrust. Therefore, the European Union considers that the response to disinformation should be based on clear political will to strengthen collective democratic resilience (European Commission 2018a).

Secondly, the European Union acknowledges the transformation in the media sector, particularly the impact of social media platforms on traditional journalism and on news media professionals, that are seeking to adapt their business models to the new reality of online news. Moreover, the EU also highlights that social media platforms have been taking a role usually associated with traditional media as content aggregators and distributors, but without the application of traditional editorial frameworks, with implications for the fact-checking of content that is disseminated. Hence, the European Union considers that there is a need to reinforce the role and quality of professional journalism and fact-checking (European Commission 2018a).

Thirdly, the European Union highlights the fundamental role that the manipulation of social media technologies has on the creation, amplification and dissemination of disinformation campaigns and also its users (European Commission 2018a).

Therefore, the EU understands that online disinformation may have multiple origins, forms and implications, thus it needs to be continuously assessed, and the response has to be adapted and calibrated to avoid symmetrical actions. Accordingly, the EU considers that the security governance of online disinformation should be done through democratic deterrence and involve measures of denial, through ignoring actions that aim to use democracy as the fundamental tool to improve societal resilience and deny interference and manipulation to succeed. At the same time, these measures are not sufficient and demand more confronting action and punishment measures that expose disinformation campaigns through refuting and reinterpreting particular events based on trustworthy sources to challenge the strategic calculus of the attacker.

In this context, the main objectives of the response to disinformation are to improve the capabilities of Union institutions to detect, analyse and expose disinformation; to strengthen coordinated and joint actions to disinformation; to mobilise the private sector to tackle disinformation; and to raise awareness and improve societal resilience (European Commission and High Representative 2018a).

In order to achieve these objectives, the EU uses a 'whole-of-society' approach that involves multiple actors in its security governance of online disinformation. European Union institutions, namely the High Representative, the European External Action Service and the European Commission, Member States, but also the private sector, particularly online platforms and the advertising industry, civil society organisations, higher education institutions, education organisations, teachers, journalists, media professionals, independent fact-checkers, academic researchers, and international partners such as NATO, G7, and OSCE.

In terms of the actions to raise awareness and improve societal resilience, the European Union understands that the users of social media are one of the main factors that contribute to the amplification of the dissemination of disinformation, which in combination with the present political and economic context creates fertile ground to be more resilient. Therefore, through actions that foster education and media and digital literacy; that support free, independent media and quality journalism; and that secure and improve resilience in the election process, the European Union aims to protect its own narrative by actively reinforcing civil society and its democratic model (European Commission and High Representative 2018a).

At the same time, the EU recognises the fundamental role of digital transition and the positive impact of technology. However, the Union also highlights the negative implications of the hostile and malicious use of technology, particularly of social media, to create, amplify and disseminate disinformation on an unprecedent scale, speed and precision. Furthermore, these platforms despite being used as a vehicle for the dissemination of disinformation, have had a limited response and have not acted proportionally and effectively to tackle this threat. Therefore, the European Union aims to build a more transparent, trustworthy and accountable ecosystem, by promoting adequate changes in platforms conduct; by promoting a more accountable information ecosystem; by enhancing the fact-checking capabilities and collective knowledge on disinformation; and by using new technologies to improve the way information is produced and disseminated online. To this end, the EU created a Code of Practice, strengthened in 2020, to promote greater transparency and accountability of online platforms, namely through the scrutiny of ad placements; the scrutiny of advertising and issue-based advertising; the promotion of the integrity of their services; the empowerment of the consumers; and the empowerment of the research community (European Commission 2021b; European Commission and High Representative 2018a).

To sum up, the security governance of online disinformation at EU level is based on a strategy of democratic deterrence that privileges measures to improve the democratic resilience of the European society rather that criminalising or prohibiting the spread of disinformation. This strategy results from the understanding of the European Union concerning the main factors that contribute to the spread and resilience of disinformation. Accordingly, the EU recognises the role that citizens play in unintentionally share false and/or misleading content, which in combination with the current political and economic context makes the spread of disinformation more successful. Hence, measures to raise awareness, enhance media literacy and to improve the resilience of European democratic societies are at centre of the action of the EU against disinformation. Moreover, the Union acknowledges the positive role of online platforms in terms of democratising the access to information, but it also recognises their use to create, disseminate and amplify disinformation. Therefore, the European Commission created an innovative tool, the Code of Practice, to commit Relevant Signatories involved in the online ecosystem to certain actions and initiatives that aim to create a safer, transparent and accountable ecosystem. Overall, the strategy of the EU against disinformation confirms the preoccupation to adopt a proportional level of reaction that do not exceed what is necessary to achieve the objectives. The EU constantly demonstrates in its discourse the preoccupation with the protection of fundamental rights and freedoms, in particular freedom of expression, and also throughout the initiatives created, that are focused on protecting freedom of expression rather than banning disinformation.

Nevertheless, the European Union assumes that these measures to improve the resilience of the European society are fundamental to deny interference and manipulation to succeed and thus to tackle disinformation, but are not sufficient and demand a more offensive posture through measures of punishment focused on confronting the disinformation narrative and expose its existence, in order to challenge the strategic calculus of the aggressor. To this end, the European Union is increasing its efforts through actions of detection, analysis and exposure of disinformation (European Commission and High Representative 2018a). But also, through democratic compellence and more recently through sanctions on Russian media.

Yet, the COVID-19 pandemic crisis demonstrated that there are some limitations related to debunking disinformation, associated with psychological bias, that if not accompanied by a strong strategic communication strategy has limited results. Moreover, despite the focus on protecting freedom of expression rather than prohibiting disinformation, recently, in the context of sanctions to Russia over Ukraine, the EU decided to suspend Russian media, which may reveal some inconsistency. These limitations and inconsistencies may be exploited by adversaries as the COVID-19 crisis demonstrated with implications for the success of the response and consequently to the protection of freedom of expression, which is the main objective in responding to disinformation.

In conclusion, the European Union considers online disinformation in security terms and normatively justifies its response based on its understanding of this type of content as a threat to the survival of the European project at all levels, at the security, political, economic and social levels. Consequently, the European Union responds to online disinformation through the strategy of democratic deterrence and at the same time considers the need to be calibrated in its actions. Accordingly, since its inception that the strategy of democratic deterrence employed by the European Union against disinformation does not involve exceptional measures and has been proportional, based on the protection and promotion of democratic principles and values and fundamental freedoms. Rather than criminalising or prohibiting online disinformation, the European Union has been designing actions that aim mostly to make the online environment more secure, transparent and accountable and by empowering its citizens. Accordingly, the response has been based on improving societal resilience through critical thinking and media literacy, strengthening quality journalism and the electoral process, and increasing the transparency and responsibility of online platforms are crucial to tackle the spread of disinformation. Furthermore, the EU uses a whole of society approach that does not only involves the EU, its institutions and Member states, but also the private sector, the media community, academia, civil society and so on. Hence, designating actors with the proper attribution and capacity to achieve the multiple objectives in the fight against disinformation. However, the limitations and inconsistencies underlying in particular the accountability of the Signatories of the Code of Practice, the limited effectiveness of debunking and the absence of a strong strategic communication policy risks being exploited by adversaries, demanding the development of more pre-emptive and accountability mechanisms. In particular, in terms of a new regulatory regime of online platforms and a strong policy of strategic communications in order to balance the effectiveness and proportionality in the security governance of online disinformation at EU level (Durach, Bârgăoanu and Nastasiu 2020; Pamment 2020; Vériter, Bjola and Koops 2020).

Therefore, we suggest that further research should consider the assessment of the implementation of the Strengthened Code of Practice 2022 in order to evaluate the implementation of the new commitments. Moreover, we also find of added value to understand why the European Union does not consider the role of traditional media as sources of disinformation, but in the context of Russia over Ukraine traditional media were suspended.

Furthermore, a deeper analysis of the work of EUvsDisinfo and how the EU has been exposing disinformation is need, in particular to evaluate the limitations of debunking strategy at EU level and if it contradicts its normative model of presenting external actors in a non-antagonistic and its implications. Furthermore, we identified that limited attention has been paid to the use of "fake news" and disinformation as a label, as a political instrument, in the European context and more research is needed.

References

ALLCOTT, Hunt, Matthew GENTZKOW. Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives.* 2017, **31**(2), pp.211-236 [consult.2022-12-18]. Available at: https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211.

ALTHUIS, Jente, Siri STRAND. Countering Fake News. In: Jente ALTHUIS, Leonie HAIDEN, eds. *Fake News: A Roadmap.* London and Riga: King's Centre for Strategic Communications (KCSC) and NATO Strategic Communications Centre of Excellence, 2018, pp.68-77 [consult.2022-12-18]. ISBN 978-9934-564-23-9. Available at: https://stratcomcoe.org/publications/fake-news-a-roadmap/137.

AVERIN, Alexander. Russia and its Many Truths. In: Jente ALTHUIS, Leonie HAIDEN, eds. Fake News: A Roadmap. London and Riga: King's Centre for Strategic Communications (KCSC) and NATO Strategic Communications Centre of Excellence, 2018, pp.59-67 [consult.2022-12-18]. ISBN 978-9934-564-23-9. Available at: https://stratcomcoe.org/publications/fake-news-a-roadmap/137.

AVERRE, Derek. Competing Rationalities: Russia, the EU and the 'Shared Neighbourhood'. *Europe-Asia Studies*. 2009, **61**(10), pp.1689-1713 [consult.2022-12-25]. Available at: https://doi.org/10.1080/09668130903278918.

BAADE, Björnstjern. Fake News and International Law. *European Journal of International Law.* 2019, **29**(4), pp.1357-1376 [consult.2022-12-18]. Available at: https://doi.org/10.1093/ejil/chy071.

BAER-BADER, Juulia. EU Response to Disinformation from Russia on COVID-19: three Lessons. *DGAP Commentary.* 2020 [consult.2022-12-26]. Available at: https://www.ssoar.info/ssoar/handle/document/69216.

BALZACQ, Thierry. Constructivism and securitization studies. In: Myriam Dunn CAVELTY, Victor MAUER, eds. *The Routledge Handbook of Security Studies*. New York: Routledge, 2010, pp.56-72.

BALZACQ, Thierry, Myriam Dunn CAVELTY. A theory of actor-network for cyber-security. *European Journal of International Security*. 2016, **1**(2), pp.176-198 [consult.2022-12-21]. Available at: doi:10.1017/eis.2016.8.

BAKIR, Vian, Andrew MCSTAY. Fake News and The Economy of Emotions: Problems, causes, solutions. *Digital Journalism.* 2017, **6**(2), pp.154-175 [consult.2022-12-18]. Available at: https://doi.org/10.1080/21670811.2017.1345645.

BARRINHA, André, Helena CARRAPIÇO. Cibersegurança. In: Raquel DUQUE, Diogo NOIVO, and Teresa de ALMEIDA E SILVA, eds. *Segurança Contemporânea.* Lisboa: PACTOR-Edições de Ciências Sociais, Forenses e da Educação, 2016, pp.245-262. ISBN 9789896930547.

BENNETT, W. Lance, Steven LIVINGSTON. The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*. 2018, **33**(2), pp.122-139 [consult.2022-12-18]. Available at: https://doi.org/10.1177/0267323118760317.

BERGER, Guy. Foreword. In: Cherilyn IRETON, Julie POSETTI, eds. *Journalism, 'Fake News' and Disinformation: Handbook for Journalism Education and Training*. Paris: UNESCO, 2018, pp.7-13. ISBN 9789231002816.

BERZINS, Janis. The new generation of Russian warfare. *Aspen Review*. 2014, **3**, pp.63-67.

BEVIR, Mark, Ian HALL. The rise of security governance. In: Mark BEVIR, Oliver DADDOW, and Ian HALL, eds. *Interpreting Global Security*. New York: Routledge, 2014, pp.17-34.

BEVIR, Mark, Oliver DADDOW, and Ian HALL. Interpreting global security. In: Mark BEVIR, Oliver DADDOW, and Ian HALL, eds. *Interpreting Global Security*. New York: Routledge, 2014, pp.1-16.

BJOLA, Corneliu. The Ethics of Countering Digital Propaganda. *Ethics and International Affairs*. 2018, **32**(3), pp.305-315 [consult.2022-12-18]. Available at: https://doi.org/10.1017/S0892679418000436.

BJOLA, Corneliu. Propaganda in the digital age. *Global Affairs*. 2017, **3**(3), pp.189-191 [consult.2022-12-19]. Available at: https://doi.org/10.1080/23340460.2017.1427694.

BJOLA, Corneliu, James PAMMENT. Digital containment: Revisiting containment strategy in the digital age. *Global Affairs*. 2016, **2**(2), pp.131-142 [consult.2022-12-18]. Available at: https://doi.org/10.1080/23340460.2016.1182244.

BOOTH, Ken. Security and emancipation. *Review of International Studies*. 1991, **17**(4), pp.313-326 [consult.2022-12-23]. Available at: http://www.jstor.org/stable/20097269.

BOSSONG, Raphael, Hendrik HEGEMANN. Internal Security. In: David J. GALBREATH, Jocelyn MAWDSLEY, and Laura CHAPPELL, eds. *Contemporary European Security.* New York: Routledge, 2019, pp.1-13. ISBN 9780415473569.

BRENNEN, Bonnie. Making Sense of Lies, Deceptive Propaganda, and Fake News. *Journal of Media Ethics*. 2017, **32**(3), pp.179-181 [consult.2022-12-19]. Available at: https://doi.org/10.1080/23736992.2017.1331023.

BUZAN, Barry. Rethinking Security after the Cold War. *Cooperation and Conflict*. 1997, **32**(1), pp.5-28 [consult.2022-12-23]. Available at: https://doi.org/10.1177/0010836797032001001.

BUZAN, Barry, Lene HANSEN. *The Evolution of International Security Studies.* Cambridge: Cambridge University Press, 2009. ISBN 9780521872614.

BUZAN, Barry, Ole WAEVER, and Jaap de WILDE. *Security: A New Framework for Analysis*. Colorado: Lynne Rienner Publishers, Inc, 1998. ISBN155587603X.

CADIER, David. The Geopoliticisation of the EU's Eastern Partnership. *Geopolitics*. 2019, **24**(1), pp.71-99 [consult.2022-12-25]. Available at: https://doi.org/10.1080/14650045.2018.1477754.

CARRAPIÇO, Helena, Benjamin FARRAND. When Trust Fades, Facebook Is No Longer a Friend: Shifting Privatisation Dynamics in the Context of Cybersecurity as a Result of Disinformation, Populism and Political Uncertainty. *Journal of Common Market Studies.* 2021, **59**(5), pp.1160-1176 [consult.2022-12-18]. Available at: https://doi.org/10.1111/jcms.13175.

CARRAPIÇO, Helena, Benjamin FARRAND. Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. *Journal of European Integration*. 2020, **42**(8), pp.1111-1126 [consult.2022-12-18]. Available at: https://doi.org/10.1080/07036337.2020.1853122.

CASIER, Tom. Are the policies of Russia and the EU in their shared neighborhood doomed to clash? In: Roger E. KANET, Maria Raquel FREIRE, eds. *Competing for Influence: The EU and Russia in Post-Soviet EURASIA*. The Netherlands: Republic of Letters Publishing, 2012, pp.31-53. ISBN 97890897990958.

CAVELTY, Myriam Dunn. Cyber-Security. In: Alan COLLINS, ed. *Contemporary Security Studies*. Fourth Edition. New York: Oxford University Press, 2016, pp.400-416. ISBN 100198708319.

CAVELTY, Myriam Dunn. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*. 2013, **15**(1), pp.105-122 [consult.2022-12-21]. Available at: https://www.jstor.org/stable/24033170.

CAVELTY, Myriam Dunn. Cyber-threats. In: Myriam Dunn CAVELTY, Victor MAUER, eds. *The Routledge Handbook of Security Studies*. New York: Routledge, 2010, pp.180-189.

CAVELTY, Myriam Dunn, Andreas WENGER. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy.* 2020, **41**(1), pp.5-32 [consult.2022-12-18]. Available at: https://doi.org/10.1080/13523260.2019.1678855.

CLEMENTS, Matthew T. Shock and awe: the effects of disinformation in military confrontation. *Policy Studies.* 2014, **35**(3), pp.211-220 [consult.2022-12-18]. Available at: https://doi.org/10.1080/01442872.2014.886679.

CHAPPELL, Laura, David J. GALBREATH, and Jocelyn MAWDSLEY. A changing security architecture. In: David J. GALBREATH, Jocelyn MAWDSLEY, and Laura CHAPPELL, eds. Contemporary European Security. New York: Routledge, 2019, pp.1-13. ISBN 9780415473569.

CHAPPELL, Laura, Jocelyn MAWDSLEY, and David J. GALBREATH. European security: where do we go from here?. In: David J. GALBREATH, Jocelyn MAWDSLEY, and Laura CHAPPELL, eds. Contemporary European Security. New York: Routledge, 2019, pp.190-201. ISBN 9780415473569.

CHRISTIANSEN, Thomas. Governance in the European Union. In: Michelle CINI, Nieves Pérez-Solórzano BORRAGÁN. *European Union Politics*. Forth Edition. Oxford: Oxford University Press, 2013, pp.103-114. ISBN 9780199694754.

CHRISTOU, George et al. European Union security governance: putting the 'security' back in. *European Security*. 2010, **19**(3), pp.341-359 [consult.2022-12-18]. Available at: https://doi.org/10.1080/09662839.2010.526109.

CINI, Michelle, Nieves Pérez-Solórzano BORRAGÁN. Introduction. In: Michelle CINI, Nieves Pérez-Solórzano BORRAGÁN. *European Union Politics*. Forth Edition. Oxford: Oxford University Press, 2013, pp.1-8. ISBN 9780199694754.

COLLINS, Alan, ed. *Contemporary Security Studies*. Second Edition. New York: Oxford University Press, 2010, ISBN 9780199548859.

CORDY, Jane. *The social media revolution: political and security implications*. NATO Parliamentary Assembly, Committee on the Civil Dimension of Security, Sub-Committee on Democratic Governance, 2017.

CORMAC, Rory, Richard J. ALDRICH. Grey is the new black: covert action and implausible deniability. *International Affairs*. 2018, **94**(3), pp.477-494 [consult.2022-12-21]. Available at: https://doi.org/10.1093/ia/iiy067.

COTTIER, Thomas et al. The Principle of Proportionality in International Law: Foundations and Variations. *Journal of World investment & Trade*. 2017, **18**, pp.628-672 [consult.2023-06-29]. Available at: https://brill.com/view/journals/jwit/18/4/article-p628_2.xml?language=en.

COTTIER, Thomas et al. The Principle of Proportionality in International Law. *Working Paper NCCR Trade Regulation Swiss National Centre of Competence in Research*. 2012, **38**, pp.1-34 [consult.2023-06-29]. Available at: https://www.wti.org/media/filer_public/9f/1b/9f1bd3cf-dafd-4e14-b07d-8934a0c66b8f/proportionality_final_29102012_with_nccr_coversheet.pdf .

CRILLEY, Rhys, Precious CHATTERJE-DOODY. Security Studies in the age of 'post-truth' politics: in defence of poststructuralism. *Critical Studies on Security*. 2018, **7**(2), pp.166-170 [consult.2022-12-19]. Available at: https://doi.org/10.1080/21624887.2018.1441634.

DAASE, Christopher, Cornelius FRIESENDORF. Introduction: security governance and the problem of unintended consequences. In: Christopher DAASE, Cornelius FRIESENDORF, eds. *Rethinking Security Governance: The problem of unintended consequences*. New York: Routledge, 2010, pp.1-20.

DANYK, Yuriy, Tamara MALIARCHUK, and Chad BRIGGS. Hybrid War: High-tech, Information and Cyber Conflicts. *Connections*. 2017, **16**(2), pp.5-24 [consult.2022-12-20]. Available at: http://www.jstor.org/stable/26326478.

DARNTON, Robert. The True History of Fake News. *The New York Review*. 2017 [consult.2022-12-23]. Available at: https://www.nybooks.com/online/2017/02/13/the-true-history-of-fake-news/.

DEIBERT, Ronald. Cyber-security. In: Myriam Dunn CAVELTY, Thierry BALZACQ, eds. *Routledge Handbook of Security Studies.* Second Edition. New York: Routledge, 2017, pp.172-182.

DELCOUR, Laure. Dealing with the elephant in the room: the EU, its 'Eastern neighborhood' and Russia. *Contemporary Politics*. 2018, **24**(1), pp.14-29 [consult.2022-12-25]. Available at: https://doi.org/10.1080/13569775.2017.1408169.

DELCOUR, Laure. The European Union: A Security Provider in the Eastern Neighbourhood? *European Security*. 2010, **19**(4), pp.535-549 [consult.2022-12-25]. Available at: https://ssrn.com/abstract=1923717.

DEL VICARIO, Michela et al. The spreading of misinformation online. *Proc Natl Acad Sci USA*. 2016, **113**(3), pp.554-559 [consult.2022-12-23]. Available at: doi: 10.1073/pnas.1517441113.

DIAS, Vanda Amaro. The EU and Russia: Competing Discourses, Practices and Interests in the Shared Neighborhood. *Perspectives on European Politics and Society*. 2013, **14**(2), pp.256-271 [consult.2022-12-25]. Available at: https://doi.org/10.1080/15705854.2013.785261.

DOOLEY, Sarah, Emma MOORE, and Alexander AVERIN. Change and 21st Century Media. In: Jente ALTHUIS, Leonie HAIDEN, eds. *Fake News: A Roadmap.* London and Riga: King's Centre for Strategic Communications (KCSC) and NATO Strategic Communications Centre of Excellence, 2018, pp.34-40 [consult.2022-12-18]. ISBN 978-9934-564-23-9. Available at: https://stratcomcoe.org/publications/fake-news-a-roadmap/137.

DURACH, Flavia, Alina BÂRGĂOANU, and Cătălina NASTASIU. Tackling Disinformation: EU Regulation of the Digital Space. *Romanian Journal of European Affairs*. 2020, **20**(1), pp.5-20 [consult.2022-12-18]. Available at: https://ssrn.com/abstract=3650780.

DUQUE, Raquel, Diogo NOIVO, and Teresa de ALMEIDA E SILVA. *Segurança Contemporânea.* Lisboa: PACTOR-Edições de Ciências Sociais, Forenses e da Educação, 2016. ISBN 9789896930547.

EGELHOFER, Jana Laura, Sophie LECHELER. Fake news as a two-dimensional phenomenon: a framework and research agenda. *Annals of the International Communication Association.* 2019, **43**(2), pp.97-116 [consult.2022-12-18]. Available at: https://doi.org/10.1080/23808985.2019.1602782.

EHRHART, Hans-Georg, Hendrik HEGEMANN, and Martin KAHL. Towards security governance as a critical tool: a conceptual outline. *European Security.* 2014a, **23**(2), pp.145-162 [consult.2022-12-18]. Available at: https://doi.org/10.1080/09662839.2013.856303.

EHRHART, Hans-Georg, Hendrik HEGEMANN, and Martin KAHL. Putting security governance to the test: conceptual, empirical, and normative challenges. *European Security.* 2014b, **23**(2), pp.119-125 [consult.2022-12-19]. Available at: https://doi.org/10.1080/09662839.2013.851676.

EHRHART, Hans-Georg, Kerstin PETRETTO. Stabilizing Somalia: can the EU's comprehensive approach work? *European Security*. 2014, **23**(2), pp.179-194 [consult.2022-12-24]. Available at: https://doi.org/10.1080/09662839.2013.856306.

EMMERS, Ralf. Securitization. In: Alan COLLINS, ed. *Contemporary Security Studies.* Second Edition. New York: Oxford University Press, 2010, pp.136-151.

ENGLE, Eric. The History of the General Principle of Proportionality: An Overview. *The Dartmouth Law Journal*. 2012, **10**(1), pp.1-11[consult.2023-06-29]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1431179.

ERIKSSON, Johan, Giampiero GIACOMELLO. The Information Revolution, Security, and International Relations: (IR)Relevant Theory? *International Political Science Review*. 2006, **27**(3), pp.221-244 [consult.2022-12-21]. Available at: https://www.jstor.org/stable/20445053.

EUNEIGHBOURS. A stronger partnership or a stronger neighbourhood [consult.2022-12-26]. Available at: https://euneighbours.eu/.

EUOBSERVER. UK, Denmark back EU counter-propaganda plan, 2015 [consult.2022-12-26]. Available at: https://euobserver.com/world/127155.

FALLIS, Don. Floridi on Disinformation. *Ethics & Politics*. 2011, **2**, pp.201-2014 [consult.2022-12-19]. Available at: https://philpapers.org/rec/FALFOD.

FARKAS, Johan, Jannick SCHOU. Fake News as a Floating Signifier: Hegemony, Antagonism and the Politics of Falsehood. *Javnost – The Public*. 2018, **25**(3), pp.298-314 [consult.2022-12-18]. Available at: https://doi.org/10.1080/13183222.2018.1463047.

FERNANDES, Sandra. The Russian Factor in the EU's Ambitions towards the East. In: Roger E. KANET, Maria Raquel FREIRE, eds. *Competing for Influence: The EU and Russia in Post-Soviet EURASIA*. The Netherlands: Republic of Letters Publishing, 2012, pp.79-104. ISBN 97890897990958.

FREIRE, Maria Raquel, Lícinia SIMÃO. The EU's security actorness: the case of EUMM in Georgia. *European Security*. 2013, **22**(4), pp.464-477 [consult.2022-12-25]. Available at: https://doi.org/10.1080/09662839.2013.808191.

GALEOTTI, Mark. Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? *Small Wars & Insurgencies*. 2016, **27**(2), pp.282-301 [consult.2022-12-21]. Available at: https://doi.org/10.1080/09592318.2015.1129170.

GERRITS, André W.M. Disinformation in International Relations: How Important Is It?. *Security and Human Rights.* 2018, **29**(1-4), pp.3-23 [consult.2022-12-18]. Available at: https://doi.org/10.1163/18750230-02901007.

GILES, Keir. *Handbook of Russian information warfare*. Rome: NATO Defense College, 2016 [consult.2022-12-19]. Available at: https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176.

GIOE, David V., Michael S. GOODMAN, and Alicia WANLESS. Rebalancing cybersecurity imperatives: patching the social layer. *Journal of Cyber Policy.* 2019, **4**(1), pp.117-137 [consult.2022-12-19]. Available at: https://doi.org/10.1080/23738871.2019.1604780.

GIUMELLI, Francesco, Eugenio CUSUMANO, and Matteo BESANA. From Strategic Communication to Sanctions: The European Union's Approach to Hybrid Threats. In: Eugenio CUSUMANO, Marian CORBE, eds. *A Civil-Military Response to Hybrid Threats*. New York: Palgrave Macmillan, 2018, pp.145-167. ISBN 978-3-319-60797-9.

GORDENKER, Leon, Thomas G. WEISS. Pluralising Global Governance: Analytical Approaches and Dimensions. *Third World Quarterly.* 1995, **16**(3), pp.357-387 [consult.2022-12-19]. Available at: http://www.jstor.org/stable/3992882.

GUESS, Andrew, Jonathan NAGLER, and Joshua TUCKER. Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances.* 2019, **5**(1), pp.1-8 [consult.2022-12-18]. Available at: 10.1126/sciadv.aau4586.

HAIDEN, Leonie. Tell me Lies, Tell me Sweet Little Lies. In: Jente ALTHUIS, Leonie HAIDEN, eds. *Fake News: A Roadmap.* London and Riga: King's Centre for Strategic Communications (KCSC) and NATO Strategic Communications Centre of Excellence, 2018, pp.7-13 [consult.2022-12-18]. ISBN 978-9934-564-23-9. Available at: https://stratcomcoe.org/publications/fake-news-a-roadmap/137.

HANSEN, Lene, Helen NISSENBAUM. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*. 2009, **53**(4), pp.1155-1175 [consult.2022-12-21]. Available at: https://www.jstor.org/stable/27735139.

HAUKKALA, Hiski. From Cooperative to Contested Europe? The Conflict in Ukraine as a Culmination of a Long-Term Crisis in EU-Russia Relations. *Journal of Contemporary European Studies*. 2015, **23**(1), pp.25-40 [consult.2022-12-25]. Available at: https://doi.org/10.1080/14782804.2014.1001822.

HEDLING, Elsa. Transforming practices of diplomacy: the European External Action Service and digital disinformation. *International Affairs.* 2021, **97**(3), pp.841-859 [consult.2022-12-18]. Available at: https://doi.org/10.1093/ia/iiab035.

HEGEMANN, Hendrik, Martin KAHL. Security governance and the limits of depoliticisation: EU policies to protect critical infrastructures and prevent radicalisation. *Journal of International Relations and Development.* 2016, **21**(3), pp.552-579 [consult.2022-12-19]. Available at: https://doi.org/10.1057/s41268-016-0078-5.

HELLMAN, Maria, Charlotte WAGNSSON. How can European states respond to Russian information warfare? An analytical framework. *European Security*. 2017, **26**(2), pp.153-170 [consult.2022-12-18]. Available at: https://doi.org/10.1080/09662839.2017.1294162.

HELM, Rebecca K., Hitoshi NASU. Regulatory Responses to 'Fake News' and Freedom of Expression: Normative and Empirical Evaluation. *Human Rights Law Review*. 2021, **21**(2), pp.302-328 [consult.2022-12-26]. Available at: https://academic.oup.com/hrlr/article/21/2/302/6129940.

HIRST, Martin. Towards a political economy of fake news. *The Political Economy of Communication.* 2017, **5**(2), pp.82-94 [consult.2022-12-19]. Available at: https://www.polecom.org/index.php/polecom/article/view/86/288.

HOFFMAN, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies, 2007.

HUMPRECHT, Edda. Where 'fake news' flourishes: a comparison across four Western democracies. *Information, Communication & Society*. 2018, **22**(13), pp.1973-1988 [consult.2022-12-18]. Available at: https://doi.org/10.1080/1369118X.2018.1474241.

HUMPRECHT, Edda, Frank ESSER, and Peter Van AELST. Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. *The International Journal of Press/Politics*. 2020, **25**(3), pp.493-516 [consult.2022-12-19]. Available at: https://doi.org/10.1177/1940161219900126.

HUYSMANS, Jef. Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security. *Alternatives*. 2002, **27**(1), pp.41-62 [consult.2022-12-23]. Available at: https://doi.org/10.1177/03043754020270S104.

IRETON, Cherilyn. Truth, trust and journalism: why it matters. In: Cherilyn IRETON, Julie POSETTI, eds. *Journalism, 'Fake News' and Disinformation: Handbook for Journalism Education and Training*. Paris: UNESCO, 2018, pp.32-43. ISBN 9789231002816.

IRETON, Cherilyn, Julie POSETTI. Introduction. In: Cherilyn IRETON, Julie POSETTI, eds. *Journalism, 'Fake News' and Disinformation: Handbook for Journalism Education and Training*. Paris: UNESCO, 2018, pp.14-25. ISBN 9789231002816.

JAKOBSEN, Peter Viggo. New threats to European security. In: David J. GALBREATH, Jocelyn MAWDSLEY, and Laura CHAPPELL, eds. *Contemporary European Security.* New York: Routledge, 2019, pp.153-172. ISBN 9780415473569.

JANKOWSKI, Nicholas W. Researching Fake News: A Selective Examination of Empirical Studies. *Javnost – The Public*. 2018, **25**(1,2), pp.248-255 [consult.2022-12-18]. Available at: https://doi.org/10.1080/13183222.2018.1418964.

JENSEN, Benjamin, Brandon VALERIANO, and Ryan MANESS. Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*. 2019, **42**(2), pp.212-234 [consult.2022-12-20]. Available at: https://doi.org/10.1080/01402390.2018.1559152.

JORGENSEN, Marianne, Louise PHILLIPS. *Discourse Analysis as Theory and Method.* London, SAGE Publications Ltd, 2002. ISBN 0761971114.

KAVALSKI, Emilian. The Complexity of Global Security Governance: An Analytical Overview. *Global Society*. 2008, **22**(4), pp.423-443 [consult.2022-12-19]. Available at: https://doi.org/10.1080/13600820802366391.

KELLO, Lucas. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*. 2013, **38**(2), pp.7-40 [consult.2022-12-21]. Available at: https://www.jstor.org/stable/24480929.

KIRCHNER, Emil J. Regional and global security: changing threats and institutional responses. In: Emil J. KIRCHNER, James SPERLING, eds. *Global Security Governance: Competing perceptions of security in the 21st century.* New York: Routledge, 2007, pp.3-22.

KIRCHNER, Emil J. The Challenge of European Union Security Governance. *Journal of Common Market Studies*. 2006, **44**(5), pp.947-968 [consult.2022-12-19]. Available at: https://doi.org/10.1111/j.1468-5965.2006.00669.x.

KIRCHNER, Emil, James SPERLING. Introduction: the EU and the governance of European security. In: Emil KIRCHNER, James SPERLING, eds. *EU security governance.* New York: Manchester University Press, 2007, pp.1-24.

KOHLER-KOCH, Beate, Berthold RITTBERGER. Review Article: The 'Governance Turn' in EU Studies. *Journal of Common Market Studies*. 2006, **44**(1), pp.27-49 [consult.2022-12-19]. Available at: https://doi.org/10.1111/j.1468-5965.2006.00642.x.

KOROSTELEVA, Elena. The Eastern Partnership Initiative: A New Opportunity for Neighbours? *Journal of Communist Studies and Transition Politics*. 2011, **27**(1), pp.1-21 [consult.2022-12-25]. Available at: https://doi.org/10.1080/13523279.2011.544381.

KRAGH, Martin, Sebastian ASBERG. Russia's strategy for influence through public diplomacy and active measures: the Swedish case. *Journal of Strategic Studies*. 2017, **40**(6), pp.773-816 [consult.2022-12-20]. Available at: https://doi.org/10.1080/01402390.2016.1273830.

KRAHMANN, Elke. Security Governance and Networks: New Theoretical Perspectives in Transatlantic Security. *Cambridge Review of International Affairs.* 2005a, **18**(1), pp.15-30 [consult.2022-12-19]. Available at: https://doi.org/10.1080/09557570500059514.

KRAHMANN, Elke. American Hegemony or Global Governance? Competing Visions of International Security. *International Studies Review*. 2005b, **7**(4), pp.531-545 [consult.2022-12-26]. Available at: https://www.jstor.org/stable/3699673.

KRAHMANN, Elke. Conceptualizing Security Governance. *Cooperation and Conflict: Journal of the Nordic International Studies Association.* 2003a, **38**(1), pp.5-26 [consult.2022-12-19]. Available at: https://doi.org/10.1177/0010836703038001001.

KRAHMANN, Elke. National, Regional, and Global Governance: One Phenomenon or Many? *Global Governance.* 2003b, **9**(3), pp.323-346 [consult.2022-12-19]. Available at: http://www.jstor.org/stable/27800486.

KURLANTZICK, Joshua. How China Ramped Up Disinformation Efforts During the Pandemic. *Council on Foreign Relations*. 2020 [consult.2022-12-24]. Available at: https://www.jstor.org/stable/resrep29835.

LA COUR, Christina. Theorising digital disinformation in international relations. *International Politics*. 2020, **57**, pp.704-723 [consult.2022-12-18]. Available at: https://doi.org/10.1057/s41311-020-00215-x.

LACY, Mark, Daniel PRINCE. Securitization and the global politics of cybersecurity. *Global Discourse*. 2018, **8**(1), pp.100-115 [consult.2022-12-21]. Available at: https://doi.org/10.1080/23269995.2017.1415082.

LAKE, David A. Rightful Rules: Authority, Order, and the Foundations of Global Governance. *International Studies Quarterly*. 2010, **54**(3), pp.587-613 [consult.2022-12-19]. Available at: http://www.jstor.org/stable/40931128.

LANGE-IONATAMISHVILI, Elina, Sanda SVETOKA. Strategic Communications and Social Media in the Russia Ukraine Conflict. In: Kenneth GEERS, ed. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015, pp.103-111.

LANOSZKA, Alexander. Disinformation in international politics. *European Journal of International Security*. 2019, **4**(2), pp.227-248 [consult.2022-12-18]. Available at: https://doi.org/10.1017/eis.2019.6.

LIAROPOULOS, A. A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia. *Journal of information Warfare*. 2015, **14**(4), pp.15-24 [consult.2022-12-21]. Available at: https://www.jstor.org/stable/26487503.

LIBICKI, Martin C. The Convergence of Information Warfare. *Strategic Studies Quarterly*. 2017, pp.49-65 [consult.2022-12-20]. Available at: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf.

LIN, Herbert. The existential threat from cyber-enabled information warfare. *Bulletin of the Atomic Scientists*. 2019, **75**(4), pp.187-196 [consult.2022-12-19]. Available at: https://doi.org/10.1080/00963402.2019.1629574.

LING, Rich. Confirmation Bias in the Era of Mobile News Consumption: The Social and Psychological Dimensions. *Digital Journalism*. 2020, **8**(5), pp.596-604 [consult.2022-12-18]. Available at: https://doi.org/10.1080/21670811.2020.1766987.

LUKITO, Josephine. Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017. *Political Communication*. 2020, **37**(2), pp.238-255 [consult.2022-12-20]. Available at: https://doi.org/10.1080/10584609.2019.1661889.

MATSABERIDZE, David. Russia vs. EU/US through Georgia and Ukraine. *Connections*. 2015, **14**(2), pp.77-86 [consult.2022-12-25]. Available at: http://www.jstor.org/stable/26326399.

MAYO, Ruth. Knowledge and Distrust May Go a Long Way in the Battle With Disinformation: Mental Processes of Spontaneous Disbelief. *Current Directions in Psychological Science.* 2019, **28**(4), pp.409-414 [consult.2022-12-18]. Available at: https://doi.org/10.1177/0963721419847998.

MCGONAGLE, Tarlach. "Fake news": False fears or real concerns?. *Netherlands Quarterly of Human Rights.* 2017, **35**(4), pp.203-209 [consult.2022-12-18]. Available at: https://doi.org/10.1177/0924051917738685.

MCMANUS, Chelsea, Celeste MICHAUD. Never Mind the Buzzwords: Defining Fake News and Post-Truth. In: Jente ALTHUIS, Leonie HAIDEN, eds. *Fake News: A Roadmap.* London and Riga: King's Centre for Strategic Communications (KCSC) and NATO Strategic Communications Centre of Excellence, 2018, pp.14-20 [consult.2022-12-18]. ISBN 978-9934-564-23-9. Available at: https://stratcomcoe.org/publications/fake-news-a-roadmap/137.

MEJIAS, Ulises A., Nikolai E. VOKUEV. Disinformation and the media: the case of Russia and Ukraine. *Media, Culture & Society.* 2017, **39**(7), pp.1027-1042 [consult.2022-12-18]. Available at: https://doi.org/10.1177/0163443716686672.

MILLER, Carl. Coronavirus: Far-right spreads Covid-19 'infodemic' on Facebook. *BBC NEWS.* 2020, [consult.2022-12-26]. Available at: https://www.bbc.com/news/technology-52490430.

MISKIMMON, Alister, Ben O'LOUGHLIN, and Laura ROSELLE. Strategic Narratives: a response. *Critical Studies on Security*. 2015, **3**(3), pp.341-344 [consult.2022-12-23]. Available at: https://doi.org/10.1080/21624887.2015.1103023.

MONSEES, Linda. 'A war against truth' – understanding the fake news controversy. *Critical Studies on Security*. 2020, **8**(2), pp.116-129 [consult.2022-12-19]. Available at: https://doi.org/10.1080/21624887.2020.1763708.

MONSEES, Linda. The Politics of Fake News – On Fake News as a Collective Symbol. In: *The Internet, Policy & Politics Conference.* Oxford, 2018.

MONTI, Matteo. The EU Code of Practice on Disinformation and the risk of the privatisation of censorship. In: Serena GIUSTI, Elisa PIRAS, eds. *Democracy and Fake News: Information Manipulation and Post-Truth Politics.* New York: Routledge, 2021, pp.214-226. ISBN 9780367479558.

MORGAN, Susan. Fake news, disinformation, manipulation and online tactics to undermine democracy. *Journal of Cyber Policy*. 2018, **3**(1), pp.39-43 [consult.2022-12-19]. Available at: https://doi.org/10.1080/23738871.2018.1462395.

MOURÃO, Rachel R., Craig T. ROBERTSON. Fake News as Discursive Integration: An Analysis of Sites That Publish False, Misleading, Hyperpartisan and Sensational Information. *Journalism Studies.* 2019, **20**(14), pp.2077-2095 [consult.2022-12-18]. Available at: https://doi.org/10.1080/1461670X.2019.1566871.

NELSON, Jacob L., Harsh TANEJA. The small, disloyal fake news audience: The role of audience availability in fake news consumption. *News Media & Society.* 2018, **20**(10), pp.3720-3737 [consult.2022-12-18]. Available at: https://doi.org/10.1177/1461444818758715.

NICOLAS, Ashley C. Taming the Trolls: The Need for an International Legal Framework to Regulate State Use of Disinformation on Social Media. *The Georgetown Law Journal Online.* 2018, **107**, pp.36-62 [consult.2022-12-18]. Available at: https://www.law.georgetown.edu/georgetown-law-journal/glj-online/107-online/taming-the-trolls/.

NIEMANN, Arne, Charlotte BRETHERTON. EU external policy at the crossroads: The challenge of actorness and effectiveness. *International Relations*. 2013, **27**(3), pp.261-275 [consult.2022-12-18]. Available at: https://doi.org/10.1177/0047117813497306.

NISSEN, Thomas Elkjer. *The Weaponization of Social Media: Characteristics of Contemporary Conflicts.* Copenhagen: Royal Danish Defence College, 2015. ISBN 9788771470987.

NITOIU, Cristian. Towards conflict or cooperation? The Ukraine crisis and EU-Russia relations. *Southeast European and Black Sea Studies*. 2016, **16**(3), pp.375-390 [consult.2022-12-25]. Available at: https://doi.org/10.1080/14683857.2016.1193305.

NITOIU, Cristian, Monika SUS. Introduction: The Rise of Geopolitics in the EU's Approach in its Eastern Neighbourhood. *Geopolitics.* 2019, **24**(1), pp.1-19 [consult.2022-12-25]. Available at: https://doi.org/10.1080/14650045.2019.1544396.

NYE, Joseph S. Jr. Soft Power and Public Diplomacy Revisited. *The Hague Journal of Diplomacy.* 2019, **14**(1,2), pp.7-20 [consult.2022-12-20]. Available at: https://doi.org/10.1163/1871191X-14101013.

NYE, Joseph S. Jr. *Cyber Power*. Cambridge: Belfer Center for Science and International Affairs, 2010.

OMAND, David. The threats from modern digital subversion and sedition. *Journal of Cyber Policy.* 2018, **3**(1), pp.5-23 [consult.2022-12-18]. Available at: https://doi.org/10.1080/23738871.2018.1448097.

ÖRDÉN, Hedvig. Deferring substance: EU policy and the information threat. *Intelligence and National Security.* 2019, **34**(3), pp.421-437 [consult.2022-12-18]. Available at: https://doi.org/10.1080/02684527.2019.1553706.

PAMMENT, James. The EU's Role in Fighting Disinformation: Taking Back the Initiative. Washington DC: Carnegie Endowment for International Peace, 2020 [consult.2022-12-26]. Available at: https://carnegieendowment.org/files/Pamment_-_Future_Threats.pdf.

PATERSON, Thomas, Lauren HANLEY. Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'. *Australian Journal of International Affairs.* 2020, **74**(4), pp.439-454 [consult.2022-12-18]. Available at: https://doi.org/10.1080/10357718.2020.1734772.

PEOPLES, Columba, Nick VAUGHAN-WILLIAMS. *Critical Security Studies: An introduction.* New York: Routledge, 2010. ISBN 0203847474.

POLYAKOVA, Alina, Daniel FRIED. *Democratic Defense Against Disinformation 2.0*. Atlantic Council Eurasia Center, 2019. ISBN 9781619775923 [consult.2022-12-18]. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/.

POPESCU, Nicu. Hybrid tactics: neither new nor only Russian. *Issue Alert, European Union Institute for Security Studies*. 2015 [consult.2022-12-21]. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_4_hybrid_warfare.pdf.

POSETTI, Julie. News industry transformation: digital technology, social platforms and the spread of misinformation and disinformation. In: Cherilyn IRETON, Julie POSETTI, eds. *Journalism, 'Fake News' and Disinformation: Handbook for Journalism Education and Training*. Paris: UNESCO, 2018, pp.57-72. ISBN 9789231002816.

POSETTI, Julie, Alice MATTHEWS. *A short guide to the history of 'fake news' and disinformation: A learning module for journalists and journalism educators*. International Center for Journalists, 2018 [consult.2022-12-19]. Available at: https://www.icfj.org/news/short-guide-history-fake-news-and-disinformation-new-icfj-learning-module.

PRIER, Jarred. Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*. 2017, **11**(4), pp.50-85 [consult.2022-12-18]. Available at: https://www.jstor.org/stable/26271634.

RAY, Argha, Joey F. GEORGE. Online Disinformation and the Psychological Bases of Prejudice and Political Conservatism. In: *Proceedings of the 52nd Hawaii International Conference on System Sciences*. 2019 Available at: http://hdl.handle.net/10125/59711.

RENZ, Bettina. Russia and 'hybrid warfare'. *Contemporary Politics*. 2016, **22**(3), pp.283-300 [consult.2022-12-21]. Available at: https://doi.org/10.1080/13569775.2016.1201316.

RHODES, R.A.W. The New Governance: Governing without Government. *Political Studies*. 1996, **44**(4), pp.652-667 [consult.2022-12-19]. Available at: https://doi.org/10.1111/j.1467-9248.1996.tb01747.x.

RID, Thomas. Cyber War Will Not Take Place. *Journal of Strategic Studies*. 2012, **35**(1), pp.5-32 [consult.2022-12-22]. Available at: https://doi.org/10.1080/01402390.2011.608939.

ROBINSON, Michael, Kevin JONES, Helge JANICKE. Cyber warfare: Issues and challenges. *Computers & Security*. 2015, **49**, pp.70-94 [consult.2022-12-21]. Available at: https://doi.org/10.1016/j.cose.2014.11.007.

ROOSE, Kevin. Get Ready for a Vaccine Information War. *The New York Times*. 2020, [consult.2022-12-26]. Available at: https://www.nytimes.com/2020/05/13/technology/coronavirus-vaccine-disinformation.html.

ROOZENBEEK, Jon, Sander VAN DER LIDEN. The fake news game: actively inoculating against the risk of misinformation. *Journal of Risk Research.* 2018, **22**(5), pp.570-580 [consult.2022-12-18]. Available at: https://doi.org/10.1080/13669877.2018.1443491.

ROSS, Andrew S., Damian J. RIVERS. Discursive Deflection: Accusation of "Fake News" and the Spread of Mis- and Disinformation in the Tweets of President Trump. *Social Media + Society*. 2018, **4**(2), pp.1-12 [consult.2022-12-18]. Available at: https://journals.sagepub.com/doi/pdf/10.1177/2056305118776010.

SARDO, Alessio. Categories, Balancing, and Fake News: The Jurisprudence of the European Court of Human Rights. *Canadian Journal of Law & Jurisprudence*. 2020, pp.435-460 [consult.2023-06-29]. Available at: https://www.cambridge.org/core/journals/canadian-journal-of-law-and-jurisprudence/article/categories-balancing-and-fake-news-the-jurisprudence-of-the-european-court-of-human-rights/2E59476A844C2245CCD4EA506C06847A.

SAURWEIN, Florian, Charlotte SPENCER-SMITH. Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe. *Digital Journalism*. 2020, **8**(6), pp.820-841 [consult.2022-12-18]. Available at: https://doi.org/10.1080/21670811.2020.1765401.

SCHIA, Niels Nagelhus, Lars GJESVIK. Hacking democracy: managing influence campaigns and disinformation in the digital age. *Journal of Cyber Policy*. 2020, **5**(3), pp.413-428 [consult.2022-12-18]. Available at: https://doi.org/10.1080/23738871.2020.1820060.

SMOUTS, Marie-Claude. The proper use of governance in international relations. *International Social Science Journal.* 1998, **50**(155), pp.81-89 [consult.2022-12-19]. Available at: https://doi.org/10.1111/1468-2451.00111.

SPERLING, James, Mark WEBBER. The European Union: security governance and collective securitization. *West European Politics*. 2019, **42**(2), pp.228-260 [consult.2022-12-19]. Available at: https://doi.org/10.1080/01402382.2018.1510193.

SPERLING, James, Mark WEBBER. Security governance in Europe: a return to system. *European Security.* 2014, **23**(2), pp.126-144 [consult.2022-12-19]. Available at: https://doi.org/10.1080/09662839.2013.856305.

SPRING, Marianna. Coronavirus: The human cost of virus misinformation. *BBC NEWS.* 2020, [consult.2022-12-26]. Available at: https://www.bbc.com/news/stories-52731624.

STEENSEN, Steen. Journalism's epistemic crisis and its solution: Disinformation, datafication and source criticism. *Journalism.* 2019, **20**(1), pp.185-189 [consult.2022-12-18]. Available at: https://doi.org/10.1177/1464884918809271.

STOKER, Gerry. Governance as theory: five propositions. *International Social Science Journal.* 1998, **50**(155), pp.17-28 [consult.2022-12-19]. Available at: https://doi.org/10.1111/1468-2451.00106.

TANDOC JR., Edson C., Zheng Wei LIM, and Richard LING. Defining “Fake News”: A typology of scholarly definitions. *Digital Journalism*. 2018, **6**(2), pp.137-153 [consult.2022-12-18]. Available at: https://doi.org/10.1080/21670811.2017.1360143.

TENOVE, Chris. Protecting Democracy from Disinformation: Normative Threats and Policy Responses. *The International Journal of Press/Politics*. 2020, **25**(3), pp.517-537 [consult.2022-12-18]. Available at: https://doi.org/10.1177/1940161220918740.

TSARUK, Oleksandr, Maria KORNIIETS. Hybrid nature of modern threats for cybersecurity and information security. *Smart Cities and Regional Development Journal*. 2020, **4**(1), pp.57-78 [consult.2022-12-20]. Available at: https://econpapers.repec.org/article/popjournl/v_3a4_3ay_3a2020_3ai_3a1_3ap_3a57-78.htm.

UCARYILMAZ, Talya. The Principle of Proportionality in Modern Ius Gentium. *Ultrecht Journal of International and European Law*. 2021, **36**(1), pp.14-32 [consult.2023-06-29]. Available at: https://utrechtjournal.org/articles/10.5334/ujiel.529.

UNDP. United Nations Development Programme. *Human Development Report 1994*. New York: Oxford University Press, 1994. ISBN 0195091701.

VAN DER MEER, Sico. Enhancing International Cyber Security: A Key Role for Diplomacy. *Security and Human Rights*. 2015, **26**(2-4), pp.193-205 [consult.2022-12-21]. Available at: https://www.shrmonitor.org/assets/uploads/2017/09/SHRS_026_02-04_Van-der-Meer.pdf.

VARGO, Chris J., Lei GUO and Michelle A. AMAZEEN. The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. *New Media & Society*. 2018, **20**(5), pp.2028-2049 [consult.2022-12-20]. Available at: https://doi.org/10.1177/1461444817712086.

VÉRITER, Sophie L., Corneliu BJOLA, and Joachim A. KOOPS. Tackling COVID-19 Disinformation: Internal and External Challenges for the European Union. *The Hague Journal of Diplomacy*. 2020, **15**(4), pp.569-582 [consult.2022-12-18]. Available at: https://doi.org/10.1163/1871191X-BJA10046.

VUORI, Juha A. Constructivism and securitization studies. In: Myriam Dunn CAVELTY, Thierry BALZACQ, eds. *Routledge Handbook of Security Studies*. Second Edition. New York: Routledge, 2017, pp.64-74.

WAEVER, Ole. Securitization and Desecuritization. In: Ronnie D. LIPSCHUTZ, ed. *On Security*. New York: Columbia University Press, 1995, pp.46-86. ISBN 9780231102704.

WAGNSSON, Charlotte, Maria HELLMAN. Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare. *Journal of Common Market Studies*. 2018, **56**(5), pp.1161-1177 [consult.2022-12-18]. Available at: https://doi.org/10.1111/jcms.12726.

WAISBORD, Silvio. Truth is What Happens to News: On journalism, fake news, and post-truth. *Journalism Studies*. 2018, **19**(13), pp.1866-1878 [consult.2022-12-18]. Available at: https://doi.org/10.1080/1461670X.2018.1492881.

WALKER, Shawn, Dan MERCEA, and Marco BASTOS. The disinformation landscape and the lockdown of social platforms. *Information, Communication & Society.* 2019, **22**(11), pp.1531-1543 [consult.2022-12-20]. Available at: https://doi.org/10.1080/1369118X.2019.1648536.

WALTZ, Kenneth N. *Theory of International Politics*. Illinois: Waveland Press, INC, 1979. ISBN 1577666704.

WANLESS, Alicia, James PAMMENT. How Do You Define a Problem Like Influence? *Journal of Information Warfare.* 2019, **18**(3), pp.1-14 [consult.2022-12-19]. Available at: https://www.jstor.org/stable/26894679.

WARDLE, Claire, Hossein DERAKHSHAN. Thinking about 'information disorder': formats of misinformation, disinformation, and mal-information. In: Cherilyn IRETON, Julie POSETTI, eds. *Journalism, 'Fake News' and Disinformation: Handbook for Journalism Education and Training*. Paris: UNESCO, 2018, pp.44-55. ISBN 9789231002816.

WEBBER, Mark et al. The governance of European security. *Review of International Studies.* 2004, **30**(3), pp.3-26 [consult.2022-12-19]. Available at: http://www.jstor.org/stable/20097896.

WENDT, Alexander. Anarchy is what states make of it: the social construction of power politics. *International Organization*. 1992, **46**(2), pp.391-425 [consult.2022-12-23]. Available at: http://www.jstor.org/stable/2706858.

WIGELL, Mikael. Democratic Deterrence: How to Dissuade Hybrid Interference. *The Washington Quarterly.* 2021, **44**(1), pp.49-67 [consult.2022-12-18]. Available at: https://doi.org/10.1080/0163660X.2021.1893027.

WIGELL, Mikael. Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy. *International Affairs*. 2019, **95**(2), pp.255-275 [consult.2022-12-18]. Available at: https://doi.org/10.1093/ia/iiz018.

WILLEMO, Jakob. *Trends and Developments in the malicious use of social media*. Riga: NATO STRATCOM COE, 2019 [consult.2022-12-20]. Available at: https://stratcomcoe.org/publications/trends-and-developments-in-the-malicious-use-of-social-media/81.

ZEITZOFF, Thomas. How Social Media Is Changing Conflict. *Journal of Conflict Resolution.* 2017, **61**(9), pp.1970-1991 [consult.2022-12-19]. Available at: https://doi.org/10.1177/0022002717721392.

ZITTRAIN, Jonathan. "Netwar": The unwelcome militarization of the Internet has arrived. *Bulletin of the Atomic Scientists*. 2017, **73**(5), pp.300-304 [consult.2022-12-25]. Available at: https://doi.org/10.1080/00963402.2017.1362907.

Sources

Commission of the European Communities. *Communication from the Commission to the Council and the European Parliament: Wider Europe – Neighborhood: A New Framework for Relations with our Eastern and Southern Neighbours*. 2003, COM(2003) 104 final, Brussels, 11 March 2003 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0104&from=EN.

Commission of the European Communities. *European Governance: A White Paper*. 2001, COM(2001) 428, 25 July 2001 [consult.2022-12-25]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/DOC_01_10.

Council of the European Union. *Council Conclusions on Security and Defence* – 2021a, 8396/21, of 10 May 2021 [consult.2022-12-25]. Available at: https://data.consilium.europa.eu/doc/document/ST-8396-2021-INIT/en/pdf.

Council of the European Union. *Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade* – 2021b, 7290/21 of 23 March 2021 [consult.2022-12-26]. Available at: https://data.consilium.europa.eu/doc/document/ST-7290-2021-INIT/en/pdf.

Council of the European Union. *Council Conclusions on media literacy in an ever-changing world*– 8274/20 of 26 May 2020.

Council of the European Union. *Council Conclusions on the strengthening of European content in the digital economy* – 14986/18 of 30 November 2018.

Council of the European Union. *Council Conclusions on Strengthening European Union-Ukraine Cooperation on Internal Security* – 15615/17 of 11 December 2017.

Council of the European Union. *Council Conclusions on developing media literacy and critical thinking through education and training* – 9641/16 of 1 June 2016.

Council of the European Union. *European Security Strategy* – 15895/03 of 8 December 2003 [consult.2022-12-25]. Available at: https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Digital Compass: the European way for the Digital Decade.* 2021a, COM(2021) 118 final, Brussels, 9 March 2021 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Commission Guidance on Strengthening the Code of Practice on Disinformation*. 2021b, COM(2021) 262 final, Brussels, 26 May 2021 [consult.2022-12-25]. Available at:

https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: On the European democracy action plan.* 2020a, COM(2020) 790 final, Brussels, 3 December 2020 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN.

European Commission. *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: on the EU Security Union Strategy.* 2020b, COM(2020) 605 final, Brussels, 24 July 2020 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future.* 2020c, COM(2020) 67 final, Brussels, 19 February 2020 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0067&from=en.

European Commission. *Commission Staff Working Document: Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement*. 2020d, SWD(2020) 180 final, Brussels, 10 September 2020 [consult.2022-12-26]. Available at: https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling online disinformation – a European Approach*. 2018a, COM(2018) 236 final, Brussels, 26 April 2018 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Securing free and fair European elections*. 2018b, COM(2018) 637 final, Brussels, 12 September 2018 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0637&from=EN.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security.* 2015, COM(2015) 185 final, Strasbourg, 28 April 2015 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0185&from=GA.

European Commission. European Digital Media Observatory (EDMO) [consult.2022-12-26]. Available at: https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory.

European Commission. The Digital Services Act package. [consult.2022-12-26]. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

European Commission and High Representative. *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade.* 2020a, JOIN(2020) 18 final, Brussels, 16 December 2020 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN.

European Commission and High Representative. *Joint Communication to the European Parliament and the Council: EU Action Plan on Human Rights and Democracy 2020-2024.* 2020b, JOIN(2020) 5 final, Brussels, 25 March 2020 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:e9112a36-6e95-11ea-b735-01aa75ed71a1.0002.02/DOC_3&format=PDF.

European Commission and High Representative. *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling COVID-19 disinformation – Getting the facts right.* 2020c, JOIN(2020) 8 final, Brussels, 10 June 2020 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0008&from=EN.

European Commission and High Representative. *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation.* 2018a, JOIN(2018) 36 final, Brussels, 5 December 2018 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0036&from=en.

European Commission and High Representative. *Joint Communication to the European Parliament, the European Council and the Council: Increasing resilience and bolstering capabilities to address hybrid threats.* 2018b, JOIN(2018) 16 final, Brussels, 13 June 2018 [consult.2022-12-26]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0016&from=GA.

European Commission and High Representative. *Joint Communication to the European Parliament and the Council: Joint Framework on countering hybrid threats – a European Union response*. 2016, JOIN(2016) 18 final, Brussels, 6 April 2016 [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

European Commission and High Representative. *Joint Communication to the European Parliament and the Council: Action Plan on Human Rights and Democracy (2015-2019) "Keeping human rights at the heart of the EU agenda".* 2015, JOIN(2015) 16 final, Brussels, 28 April 2015 [consult.2022-12-26]. Available at: https://reliefweb.int/report/world/action-plan-human-rights-and-democracy-2015-2019-keeping-human-rights-heart-eu-agenda.

European Council. *European Council special meeting conclusions*. 2020, Brussels, 2 October 2020 [consult.2022-12-26]. Available at: https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf.

European Council. *European Council meeting conclusions*. 2019, Brussels, 22 March 2019 [consult.2022-12-26]. Available at: https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/en/pdf.

European Council. *European Council meeting conclusions*. 2018, Brussels, 28 June 2018 [consult.2022-12-25]. Available at: https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf.

European Council. *European Council meeting conclusions*. 2017a, Brussels, 23 June 2017 [consult.2022-12-26]. Available at: https://www.consilium.europa.eu/media/23985/22-23-euco-final-conclusions.pdf.

European Council. *European Council meeting conclusions*. 2017b, Brussels, 19 October 2017 [consult.2022-12-26]. Available at: https://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf.

European Council. *European Council meeting conclusions*. 2015, Brussels, 19 and 20 March 2015 [consult.2022-12-25]. Available at: https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf.

European Council and Council of the European Union. EU restrictive measures against Russia over Ukraine (since 2014) [consult.2022-12-26]. Available at: https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/.

European External Action Service. Questions and Answers about the East StratCom Task Force [consult.2022-12-26]. Available at: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11233.

European Parliament. *Resolution on EU strategic communication to counteract propaganda against it by third parties* (2016/2030(INI)), 23 November 2016. [consult.2022-12-25]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016IP0441&from=EN.

European Union. *A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security*, 2022a [consult.2022-12-26]. Available at: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en.

European Union. *The Strengthened Code of Practice on Disinformation*, 2022b [consult.2022-12-26]. Available at: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

European Union. *A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and* *security*, 2022a [consult.2022-12-26]. Available at: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en.

European Union. *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign and Security Policy*. 2016 [consult.2022-12-25]. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/EUGS_0.pdf.

European Union. *Code of Practice on Disinformation*, 2018 [consult.2022-12-26]. Available at: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

European Union. *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union* (Lisbon), 2009, Official Journal of the European Union [consult.2022-12-26]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=EN.

High Representative. *Action Plan on Strategic Communication*. 2015, Ref.Ares(2015)2608242, 22 June 2015 [consult.2022-12-25]. Available at: https://www.eeas.europa.eu/sites/default/files/action_plan_on_strategic_communication.docx_eeas_web.pdf.

Secretary-General of the United Nations. *Report on Countering disinformation for the promotion and protection of human rights and fundamental freedoms.* 2022, A/77/287, 12 August 2022 [consult.2023-06-29]. Available at: https://digitallibrary.un.org/record/3987886#record-files-collapse-header.