



Universiteit
Leiden
The Netherlands

Countering misinformation in the EU: origins, evolution, and prospects

Vériter, S.L.

Citation

Vériter, S. L. (2025, June 3). *Countering misinformation in the EU: origins, evolution, and prospects*. Retrieved from <https://hdl.handle.net/1887/4247700>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/4247700>

Note: To cite this publication please use the final published version (if applicable).

The true splendour of science is not so much that it names and classifies, records and predicts, but that it observes and desires to know the facts, whatever they may turn out to be.

— Allan Watts, *The Wisdom of Insecurity*

Introduction

This dissertation seeks to expand knowledge about misinformation and governmental responses to this phenomenon by examining *why European Union counter-misinformation policies emerged the way they did, how they have evolved, and the lessons about information governance deriving from this case study*¹. It is based on five separate publications that address these questions from different angles further detailed in this Introduction. On the one hand, the thesis explores the complexity of **information challenges** commonly described as fake news, mis- and disinformation, information warfare, or information manipulation and interference. On the other hand, it analyses related **policy responses**, with a focus on the European Union (EU) given its growing interest in the field and its capacity to set global standards and policies. The dissertation explores the background of EU counter-misinformation measures: the problem(s) they seek to address, the context of their adoption, the key political actors driving their development, and the procedures used to bring policies to fruition. From this analysis, the thesis derives theoretical, ethical, and practical conclusions, using the EU case to draw broader lessons about information challenges, their interpretation as security threats, and their governance. These issues are of paramount importance for the field of International Relations because they dramatically affect one of the pillars of liberal democracy, the information ecosystem on which rests its public sphere.

The thesis makes both a theoretical and empirical contribution to the field of International Relations, in particular Diplomatic and European Studies. First, it makes a theoretical contribution because it **deepens our understanding of information challenges**, by shining light on what leads them to become prominent subjects of concern for political actors such as the EU. By studying the processes that lead to new counter-misinformation measures (e.g. new policies and regulations), the thesis critically assesses the nature of the problem(s) they are designed to tackle. Ultimately, it proposes a new approach to information challenges that recognises their complexity and global nature. Second, it makes an empirical contribution by **uncovering three milestones** in the development of EU policy measures: (1) Russia's illegal annexation of Crimea and the subsequent creation of the East StratCom Task Force, (2) the COVID-19 pandemic outbreak and the subsequent strengthening of EU crisis response mechanisms, and (3) Russia's invasion of Ukraine and the EU's subsequent broadcasting ban on Russian state-sponsored media *RT* and *Sputnik*. It deconstructs those responses in detail, revealing the dynamics and actors that underpin them, and the challenges encountered along the way, such as policy contestation and contradictions.

The dissertation is structured as follows. First, the rest of this Introduction (a) explains why this a significant topic of research from both scholarly and policy-oriented perspectives, (b) introduces the case study and research questions, (c) discusses the relevant literature in this field, (d) unpacks the research questions and the methods used to answer them, and (e)

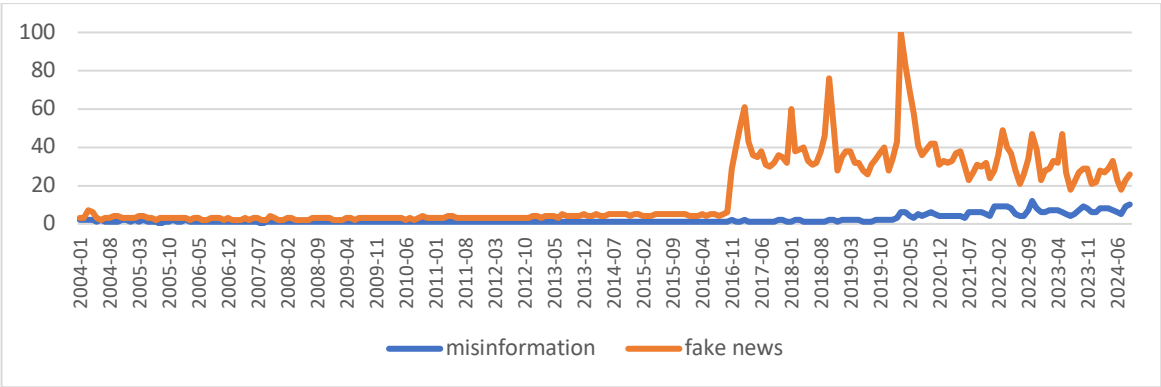
¹ The central research questions are elaborated and detailed in the Research Design section of this Introduction.

provides an overview of the chapters and how they each contribute to the questions. Then, [Part I](#) contains one chapter that makes important conceptual clarifications about information challenges. [Part II](#) contains three chapters that analyse the responses to the abovementioned milestones in EU counter-misinformation, discussing the development of this policy field. Based on this analysis, [Part III](#) consists of one chapter that presents an innovative approach to understanding and responding to information challenges. The [Conclusion](#) summarise the empirical and theoretical findings, as well as avenues for further research and better practices.

1. Significance of Misinformation Policy Research

Misinformation—inaccurate or misleading information—has unmistakably become a ubiquitous topic of concern for security and global affairs. In 2014, the world witnessed “little green men” illegally annex Crimea (Russian soldiers who, without identifying insignia, took control of the Ukrainian peninsula). Russian President Putin initially denied responsibility for this but later acknowledged it². The confusion and surprise resulting from this violation of international law and the lies that accompanied it led to a stark awakening among the West. It marked a critical juncture for European foreign policy, reignited great power tensions, and exposed the limitations of liberal international institutions in maintaining geopolitical stability³. Further concerns about modern information warfare and the potential dangers of online misinformation emerged, for instance following the 2019 Mueller report unveiling Russia’s large-scale campaigns to influence the 2016 US presidential election⁴, or with the widespread vaccine misinformation during the COVID-19 pandemic⁵.

Table 1: Evolution of interest in “misinformation” and “fake news” on Google⁶



Source: Google Trends, 2024

² Paul and Matthews 2016, 8.

³ Ikani 2019; Juncos and Pomorska 2021; MacFarlane and Menon 2014; Mearsheimer 2014.

⁴ US Department of Justice 2019.

⁵ Gabarron, Oyeyemi, and Wynn 2021.

⁶ The results indicate the proportion of searches for a particular keyword, relative to the region with the highest usage rate for that keyword. A value of 50 indicates that the keyword was used half as frequently, while a value of 0 signifies insufficient data for that keyword. Google Trends 2024.

While misinformation and information warfare are not new, the Information and Communication Technology (ICT) Revolution have transformed their practice. With the emergence and development of the internet and social media, state and non-state actors can disseminate information more rapidly and widely. This shift from traditional media to digital platforms enables more sophisticated targeting, real-time engagement, and greater anonymity, making it easier to influence public opinion or sow confusion internationally⁷. The design of online platforms contributes to the spread of misinformation, with algorithms that make sensational content go viral⁸. “Fake news” is how misinformation became popularised, as illustrated by its designation as Word of the Year in 2017 and the sharp increase in its usage over the last decade, shown in [Table 1](#)⁹. With the recent rise of Artificial Intelligence (AI) and the large-scale automated communications it enables, this issue has become even more prominent, although scholars argue that fears over this new technology are overblown¹⁰.

Misinformation has become a prominent subject of interest in politics and governance¹¹. Between 2011 and 2022, 78 countries passed legislation to limit the spread of misinformation online, with varying approaches ranging from criminalising its creation and distribution to increasing transparency requirements¹². Criticism emerged regarding the negative impact that counter-misinformation policies and regulations may have on fundamental freedoms and liberal democratic values, especially free speech¹³. In authoritarian regimes, counter-misinformation measures are used to suppress dissenting voices and silence opposition¹⁴. Indeed, misinformation is often presented as a matter of security, sometimes justifying exceptionally strong responses, which raises important questions about the balance between preserving political and public interests, between strategic advantage and individual freedoms.

Simultaneously, misinformation has gained prominence as a subject of scientific inquiry. A vast literature explores the spread of false reports, intentional and strategic or not, and the formation of erroneous beliefs¹⁵. More than 129,000 publications mentioned “fake news” in their title between 2015 and 2023, according to Google Scholar. In comparison, “online news” yields about 90,700 results for the same period. In their landmark report *Information Disorder*, Wardle and Derakhshan provided an influential baseline to understand those challenges and their potential solutions¹⁶. Since then, scholars have vastly explored their nature and scope¹⁷.

⁷ Marwick and Lewis 2017; Ruffo et al. 2021.

⁸ Narayanan 2023.

⁹ Sauer 2017.

¹⁰ Simon, Altay, and Mercier 2023.

¹¹ Freelon and Wells 2020; Neo 2021; Saurwein and Spencer-Smith 2020.

¹² Lim and Bradshaw 2023.

¹³ Mchangama 2022a; Nielsen 2021.

¹⁴ Silenced and Misinformed 2021; V riter et al. 2021.

¹⁵ Ecker et al. 2022; Kapantai et al. 2021; Murphy et al. 2023.

¹⁶ Wardle and Derakhshan 2017.

¹⁷ See Bjola and Pamment 2019; Bradshaw and Howard 2019; Freelon and Wells 2020; Lanoszka 2019; Miskimmon, O’Loughlin, and Roselle 2013; Surowiec and Manor 2021.

However, while the volume of research on misinformation increased, the field remains fragmented and lacks meta-frameworks integrating findings across disciplines. It faces ethical, normative, and methodological issues tempering its credibility and relevance¹⁸, leading some experts to call for the entire field to stop because it brings scholars into “hopelessly subjective territory”¹⁹. A common argument amongst critiques is that misinformation is exaggerated as a policy issue and utilized to serve political agendas, often scapegoating external actors to deflect from internal shortcomings²⁰. It is therefore particularly important to analyse the background of counter-misinformation policies to better understand their development, the purpose they serve, and their implications for socio-political life.

2. Case Study: EU Response to Information Challenges

Europe and North America have been at the forefront of initiatives related to information challenges²¹. Over the last decade, the European Union (EU) has developed far-reaching responses based on a detailed and extensive legal framework and a multi-level governance apparatus²². Some of the most prominent EU measures in this field include the Digital Services Act, the Disinformation Code of Practice, and a ban on Russian state-sponsored media outlets²³ (see [Annex G](#) for a chronological overview of key measures). The EU has been recognised as a global standard-setter in policy areas like data protection, consumer rights, and environmental regulations, also known as the *Brussels effect*²⁴. In the digital sphere as well, the EU has the potential to influence regulations and discussions about information challenges worldwide²⁵. The EU thus offers a great case study for a dissertation on counter-misinformation policies due to its far-reaching approach and significance as a global actor in this area.

Before introducing the EU’s approach to information challenges and the questions that it raises in the context of this dissertation, it is useful to review the basic tenets of EU policymaking. EU policies are divided into exclusive and shared competences, based on the areas of authority assigned by the Treaty on the Functioning of the European Union. For exclusive competences, the EU has full authority to legislate, leaving little to no room for Member State intervention. These areas include competition policy, trade policy, and the single market. In contrast, shared competences allow both the EU and Member States to legislate, although Member State action is secondary to EU regulations in the same policy domain. Shared competences cover areas like environmental policy, energy, and public health, allowing the EU to coordinate these efforts. For policy areas that are neither shared nor exclusive to the EU (i.e. where member

¹⁸ Altay, Berriche, and Acerbi 2023; Camargo and Simon 2022; Murphy et al. 2023.

¹⁹ Shapiro and Norton 2024.

²⁰ Belogolova et al. 2024; Camargo and Simon 2022; Wilde 2022.

²¹ Smith 2020.

²² Pamment 2020a; LupaMundi 2024; Smith 2020.

²³ Ördén 2019.

²⁴ Bradford 2020.

²⁵ Bendiek and Stürzer 2022; Bueno and Canaan 2024; Nunziato 2023.

states have the sole legislative authority), so-called ‘supporting competences’ come into play. In these areas, the EU can only intervene to support, coordinate, or supplement Member State policies rather than legislating directly.²⁶ This means the EU has no authority to harmonize national laws but can fund and coordinate initiatives to help Member States achieve common objectives. Examples include education, culture, and tourism.²⁷

The EU uses different legislative procedures based on this categorisation. For exclusive and shared competences, the ordinary legislative procedure (OLP) typically applies, requiring co-decision between the European Parliament and the Council of the EU (“the Council”). In policy areas of supporting competences, special legislative procedures may apply, often involving consultation with the Council or the Parliament. The Common Foreign and Security Policy (CFSP) requires a different and separate process: all Member States must agree unanimously, reflecting national sovereignty in foreign policy. The making of a joint foreign or security measure typically happens in three steps. First, Member States communicate their position, interests, and objectives within the European Council and the various configurations of the Council and its preparatory bodies, where the bulk of the work is done ahead of ministerial meetings. Second, proposals are discussed in the relevant preparatory bodies and working groups, including the Committee of Permanent Representative II (COREPER II), the Political and Security Committee (PSC), the Working Party on Eastern Europe and Central Asia (COEST), the Working Party on Information, and the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats. Further upstream, the Antici Group and the Nicolaïdis Group respectively prepare the work for COREPER II and PSC meetings. Third, the Council can adopt CFSP decisions and regulations in its various configurations, typically the General Affairs Council, chaired by the Presidency of the Council, and the Foreign Affairs Council, chaired by the HRVP.²⁸ Responses aimed to tackle misinformation fit in a wide variety of thematic policy discussions, from media policy to foreign and security policy.

Having clarified the essential aspects of EU policymaking, especially for foreign and security policies, the remainder of this section outlines the pillars of the EU’s approach to information challenges, the surprising elements it reveals, as well as the questions that derive from it. It starts by looking at the EU’s discourse on information challenges and clarifying some of the key terms used in this dissertation. It then briefly reviews the evolution of EU counter-misinformation policies, from their inception to their current state, explaining the added value of this case study for scholarly and policy debates about information challenges.

The EU’s discourse related to information challenges initially focused on “disinformation”, i.e. incorrect or misleading information shared with the intention to cause harm²⁹, but has since then shifted towards “Foreign Information Manipulation and Interference” (FIMI) and the

²⁶ *Treaty on the Functioning of the European Union* 2012, art. 6.

²⁷ *Ibid.*, art. 2.

²⁸ *Ibid.*, arts. 205–222, 289, 294; *Treaty on European Union* 2012, arts. 21–46.

²⁹ Wardle and Derakhshan 2017.

protection of European democracy. This reflects a changing understanding of the issues the EU seeks to address with its counter-misinformation measures—issues I refer to collectively as “information challenges”. One of the arguments of this dissertation is that the concept of “disinformation” is flawed, because it rests upon the assumption that intent can be objectively defined, when it is in fact intersubjective. Its definition depends on shared social and political understandings of intent and harm within a given community or context. This dissertation thus uses the term “misinformation” preferentially, without assumption about intent or harm.

[Chapter 1](#) makes important conceptual clarifications about information challenges (see Table 2 for an overview of key terms), offering a framework for analysing the global, political, and societal impact of information challenges, while discussing tools for international cooperation. Information challenges are highly influenced by political actors and structures, hence the usefulness of International Relations and diplomatic studies to better understand them, in addition to History, Psychology, and Computer Science, to cite a few other disciplines that offer complementary perspectives.

In 2015, the first joint EU measure against misinformation emerged: the East StratCom Task Force (ESTF). The ESTF consists of a unit within the European External Action Service (EEAS). The EEAS is equivalent to a European Foreign Affairs Ministry and headed by the High Representative / Vice-President of the European Commission (HRVP)³⁰. The ESTF’s mandate was to counter pro-Kremlin disinformation through strategic communication and public diplomacy, fact checking, and support for independent media³¹. While responding to Russian propaganda is now a central concern for most EU states, it was not the case at the time of the ESTF’s creation: it was a contentious subject for policymakers wary of undue interference on free speech³² and Member States were divided about their relations towards Russia³³. Yet, it is in this context that the first European measure against misinformation emerged, in a policy area requiring Member States’ unanimity, the CFSP. Those joint measures even preceded most national policies of the kind in the EU. This leads to the first key research question of this dissertation: *why did EU counter-misinformation policies emerge the way they did?* [Chapter 2](#) explains that the team was put together upon the initiative of the Baltic states, particularly affected by pro-Kremlin propaganda in the aftermath of the 2013-14 Ukraine crisis, given their proximity to the conflict and large Russian-speaking population. The chapter explains how such small states could have long-lasting influence in the EU.

Information challenges gained further prominence in the EU, for example following the Macron leaks, part of a broader Kremlin operation to influence the 2017 French election³⁴, and the 2018 Cambridge Analytica Scandal, which involved the misuse of personal data to influence political campaigns, raising fears of foreign interference at the dawn of the 2019

³⁰ Duke 2013; Smith 2013; Vanhoonacker and Pomorska 2013.

³¹ EEAS 2015.

³² Vilson 2016.

³³ MacFarlane and Menon 2014; Croft and Emmott 2014.

³⁴ Jeangène Vilmer 2019.

European Parliament elections³⁵. The crises triggered by the COVID-19 pandemic and the 2022 invasion of Ukraine deepened feelings of uncertainty and fear, as well as concerns about the negative effects of misinformation on European stability and security. A study led by Devaux et al. at RAND shows that, because of misinformation, there is increasing disagreement and uncertainty about facts as well as decreasing engagement in civic life in Europe³⁶. However, there is also increasing confusion about misinformation and its effects, including in scholarly circles, as well as growing scrutiny over the appropriateness of policy responses³⁷. This leads to the second key research question of this dissertation: *how have EU counter-misinformation policies evolved since their inception?* Chapter 3 examines the EU's response to the “infodemic” that accompanied the 2020 pandemic outbreak, highlighting challenges for its internal public sphere and its geopolitical power on the global stage. Chapter 4 delves into the EU's broadcasting ban on Russian state-sponsored media, implemented in response to Russia's invasion of Ukraine in February 2022. It argues that the EU's collective securitisation of “disinformation”, i.e. its social construction as a security threat, is what allowed for such an unprecedented measure.

The case of EU counter-misinformation policies has far-reaching implications for the study and practice of European foreign and security policy, digital governance, strategic communication, and information governance (the management of information dynamics that may present risks to public security, public health, or political stability)³⁸. Indeed, the effects of EU policies and regulations extend far beyond Europe, with important consequences for private companies across the world, including fines up to 6% of annual turnover if they fail to comply³⁹. This creates normative risks affecting public spheres within and beyond Europe. First, the EU's approach could fuel the perception that governments are seeking to expand control over the public and the flow of information, a view that has gained prominence since the COVID-19 pandemic⁴⁰. This can drive users to turn to less regulated, harder-to-monitor alternative platforms, while also deepening distrust in public institutions⁴¹. Second, political pressure and legal obligations may lead online platforms to over-censor content to avoid risks, often relying on their own terms of services and community guidelines as the basis to moderate undesirable content. Civil society organisations and legal experts have criticised those measures, arguing that they substitute democratic lawmaking and judicial processes with privatized, unaccountable systems that negatively impact the public sphere⁴². This therefore begs the question: *which lessons about information governance we can draw from this case study?*

³⁵ European Parliament 2018.

³⁶ Devaux, Grand-Clement, and Hoorens 2022.

³⁷ Altay, Berriche, and Acerbi 2023; Camargo and Simon 2022; Shapiro and Norton 2024.

³⁸ Epstein 2013.

³⁹ Espinoza 2024; Goujard 2024; Lee Myers 2023; Vériter 2023.

⁴⁰ Lim and Bradshaw 2023.

⁴¹ Vériter 2021.

⁴² Chang 2018; Mchangama 2022b; Persily and Tucker 2020, 209–210 and 224–226.

On the one hand, this case study provides a comprehensive overview of a fast-growing and fragmented policy field, as well as practical avenues to enhance it. Looking into the EU's approach to counter misinformation brings clarity to the factors that have influenced EU policymaking in this field. It makes both an empirical and theoretical contribution to the field of European studies, by considerably expanding knowledge of EU counter-misinformation policies and their background, what this can tell us about the EU as an actor in this realm, as well as refining theories and concepts used to explain their development, such as securitisation theory. The thesis also discusses some of the shortcomings of the EU's approach, in terms of effectiveness and ethical or normative value, with practical takeaways to address them. [Chapter 2](#) focuses on the origins of EU counter-misinformation policies with the creation of the ESTF in 2015, while [Chapter 3](#) discusses the EU's response in the context of the COVID-19 pandemic and [Chapter 4](#) examines one of the latest developments in EU counter-misinformation, the broadcasting ban of Russian state-sponsored media *RT* and *Sputnik* in the aftermath of Russia's invasion of Ukraine. Collectively, the thesis thus offers a detailed empirical and theoretical analysis of three milestones in EU counter-misinformation.

On the other hand, unpacking the adoption of EU counter-misinformation measures brings clarity about the nature of the problem they seek to address. By analysing who is involved and their motivations, we can discern how the problem is being framed (e.g. as a security threat, a public health issue, a democratic crisis) and which interests are being protected. This deepens our understanding of information challenges, as it explains how they are understood in the political sphere, where they are primarily articulated and tackled⁴³. The EU being a prominent legislator in the field of misinformation, with important effects beyond the region, it offers a great case study to understand the conceptualisation of information challenges in a broader, global sense. [Chapter 1](#) provides initial conceptual clarifications related to information challenges and their governance, from the perspective of diplomatic studies but integrating insights from History, Psychology and Computer Science. Building on the analysis of the EU case and the shortcomings it highlighted, the final [Chapter 5](#) proposes a new way of conceptualising information challenges and their governance, drawing on complexity theory and deriving insights and methods from theoretical physics and statistical mechanics.

The [Research Design](#) section of this introduction further unpacks the key research questions of the dissertation, the sub-questions they raise, the gaps they seek to address, and the methods used to answer them. Before that, the following section provides an overview of the literature relevant for the research questions and identifies key debates and gaps, from scholarly and policy perspectives.

⁴³ Cipers, Meyer, and Lefevre 2023; Nielsen 2024.

3. Literature Review

This dissertation builds on literature ranging from International Relations and Diplomacy to Psychology and Computer Science. Information challenges are at the crossroads between technology, politics, and security. It is precisely their convoluted nature which makes them difficult to comprehend and address. The sheer volume of research conducted on the subject, heavily driven by policy concerns, contributes to fragmentation and confusion⁴⁴. This literature review provides a summary of the state of the field, its key findings and gaps, later expanded in the relevant chapters of the thesis. It is structured in five parts. First, it examines scholarship that seeks to define information challenges, identifying shortcomings for both research and policy. Second, it reviews the history of information challenges, how they have evolved and been studied. Third, it considers contemporary perspectives on information challenges, looking at knowledge of their causes and effects as well as appropriate responses. Fourth, it delves into the background of the EU's approach to information challenges and how it has been theorised in the literature, finding gaps and opportunities for further elaboration. Finally, a brief summary provides an overview of the strengths and weaknesses of the literature relevant for this research project, which breadth reflects its complexity.

3.1 Defining Information Challenges

First and foremost, a vast literature aims to provide conceptual clarity with regards to information challenges. To make sense of these phenomena, scholars have used various concepts (e.g. propaganda, public diplomacy, information warfare, misinformation, but also framing and strategic communication, to cite a few) and have drawn from several disciplines and fields (e.g. International Relations, diplomatic studies, communication studies, Psychology, Computer Science, History, linguistic studies)⁴⁵. Kapantai et al. give a taxonomical framework and a glossary clarifying key terms, from “click-bait” content and “pseudoscience” to “trolling” and “conspiracy theories”⁴⁶.

In their 2017 report *Information Disorder*, Wardle and Derakhshan provided an influential baseline to understand information challenges and appropriate responses⁴⁷. They conceptualise “information disorders” based on two dimensions—harm and falseness—and consider three elements—agent, message, and interpreter—as a matrix to differentiate between misinformation, disinformation, or malinformation⁴⁸. Wardle and Derakhshan's framework has been widely used as a point of reference in the scientific literature on information challenges,

⁴⁴ Altay, Berriche, and Acerbi 2023; Camargo and Simon 2022.

⁴⁵ See, for example: Bially Mattern 2005; Bjola and Manor 2024; Bjola and Pamment 2019; Lecheler and Vreese 2018; Melissen 2011; Miskimmon, O'Loughlin, and Roselle 2013; Nye 2004; Tay et al. 2024; van der Linden 2023.

⁴⁶ Kapantai et al. 2021.

⁴⁷ Wardle and Derakhshan 2017.

⁴⁸ Ibid., 5.

totalling over 3500 citations at the time of writing⁴⁹. It has also influenced key policy documents on the subject. For example, the 2018 EU *Report of the independent High-level Group on fake news and online disinformation*, which led to the EU's Action Plan Against Disinformation and the Code of Practice on Disinformation, notably used Wardle and Derakhshan's conceptual framework as a reference to formulate policy recommendations⁵⁰. The United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression also used it as a central point of reference in their report on disinformation and freedom of opinion and expression⁵¹.

While Wardle and Derakhshan's framework offers a simple categorization, it fails to capture the non-binary nature of information and does not help understanding what constitutes "information order" as opposed to the "disorders" it defines. Information is rarely simply true or false, as it is most often presented as part of stories or frames of references that create nuance. Information is neither simply harmful or safe, since harm can be intersubjective, sometimes invisible, and difficult to measure. Thus, this framework, although influential, does not help to understand where to draw the line between what it considers to be problematic (disorder) and what is not (order). Because of the vagueness of those dimensions, it becomes easy to qualify undesirable information as "disorder" or "disinformation", leading to conceptual stretching and weak analytical utility. One of the arguments of this dissertation is thus that the concept of "disinformation" is fundamentally flawed, because it rests upon the assumption that intent can be objectively defined, when it is in fact intersubjective and complex⁵². Intent also seldom matters since we know that misinformation is a collaborative process that engages gullible, well-intended folks as much as malicious ones⁵³. This dissertation suggests preferentially using the terms "misinformation" and "information challenges", devoid of assumptions about intent or binary conceptions of information. This has the advantage of providing a more objective and scientific approach to understanding information challenges, as well as enhances prospects of international cooperation. Removing intersubjective dimensions allows for concepts that have analytical value independently of the observer, hence creating prospects for easier understanding and collaboration across silos.

Other conceptual frameworks categorise information based on interpretation, deception, or receptivity⁵⁴, but still lack clear distinctions between what is considered problematic and what is not, a fine line that is impossible to define with certainty. Whether it is Amazeen's Recognition and Response Model⁵⁵ or the Reliability-weighting Process of Zmigrod, Burnell,

⁴⁹ See Amazeen 2023, 1; Bennett and Livingston 2021, 192; Gradoń et al. 2021, 2; Lazer et al. 2018b; Jayakumar, Ang, and Diyanah Anwar 2020, 7.

⁵⁰ HLEG 2018, 10.

⁵¹ Khan 2021.

⁵² Grammont, Legrand, and Livet 2010.

⁵³ Starbird, Arif, and Wilson 2019.

⁵⁴ See Amazeen 2023; Chadwick and Stanyer 2022; Pamment 2020b; Zmigrod, Burnell, and Hameleers 2023.

⁵⁵ Amazeen 2023.

and Hameleers⁵⁶, many conceptualisations rest upon information's coherence with one's own beliefs or knowledge as the fundamental characteristic of misinformation. Those frameworks, classifying information based on appropriateness, are often biased because this is an inherently relational exercise, therefore tainted by worldviews and belief systems. This may explain why misinformation studies have been driven by policy-oriented work⁵⁷: they often reflect political perspectives and thus risk furthering polarisation rather than addressing it. Another branch of research focuses on characterising information challenges based on deceptive intentions⁵⁸ which, as mentioned above, can seldom be determined with certainty and objectivity. In sum, more research is needed to understand information dynamics and the danger they can pose *beyond* belief systems and political silos, focusing on the information environment as a whole⁵⁹. Global and apolitical perspectives on information ecosystems are needed, both for the scholarly development of this field and for the elaboration of sound policy solutions.

3.2 The History of Information Challenges and their Study

Looking at the history of information challenges contributes to knowledge about contemporary issues by offering insights into their evolution, patterns or shifts in their key drivers and responses, and how they are being studied and talked about. It helps to identify long-term trends and understand root causes. By examining how information challenges have been addressed and studied, we can thus better anticipate future challenges and develop more robust, contextually aware theoretical frameworks and responses. Above all, historical perspectives showcase that the problems arising from erroneous beliefs and how they are weaponized for power are far from new. While the methods have evolved—with the ICT Revolution making information easier to weaponize and more pervasive—the underlying dynamics remain familiar: seeking influence and power to protect one's perceived interests.

The term “propaganda” originated in the Reformation period (17th century), describing the Roman Catholic Church's efforts to promote Catholic doctrine in response to Protestant influence through the Congregation for the Propagation of the Faith⁶⁰. It then gained a pejorative meaning as a result of Nazi propaganda, which cemented its association with mass manipulation and control, often intertwined with authoritarian regimes⁶¹. The scientific study of information challenges emerged in the mid-20th century, largely driven by the role of propaganda in the context of World War I and II. Scholars like Lasswell pioneered early communication studies, focusing on how governments use information campaigns to influence public opinion and mobilize populations for war⁶². Lasswell's model “Who says

⁵⁶ Zmigrod, Burnell, and Hameleers 2023.

⁵⁷ Camargo and Simon 2022.

⁵⁸ Chadwick and Stanyer 2022.

⁵⁹ Floridi 2014; Shapiro and Norton 2024.

⁶⁰ Cull, Culbert, and Welch 2003, xvi.

⁶¹ Ibid., xv.

⁶² Lasswell 1938; Lasswell 1958.

what, to whom, in which channel, with what effect?” established the groundwork for analysing influence, messaging strategies, and public persuasion, revealing how information affects public sentiment, reinforces norms, and shapes power structures⁶³. The concepts of strategic communications and strategic narratives further contributed to this literature by explaining the use of discourse (through language, context, and social practices) as an instrument of power in global affairs⁶⁴.

In the mid-20th century, propaganda was closely tied to national security and foreign policy because state-sponsored influence campaigns emerged as a central feature of geopolitical strategy, hence the rise of International Relations (IR) and diplomatic studies to understand those phenomena. Nye’s concept of soft power highlighted the critical role that information plays in diplomatic relations, as states increasingly sought influence through persuasion rather than coercion⁶⁵. The “framing” of certain policies and ideas became the subject of scientific enquiry in linguistics, media, and political studies⁶⁶. At the same time, securitisation theory was first conceptualized by the Copenhagen School, arguing that issues become security matters not because they inherently are threats, but because they are presented as such by influential actors (like political leaders or the media), thereby justifying extraordinary countermeasures often outside of normal democratic processes⁶⁷. IR scholars tend to agree that misinformation and information warfare are significant disruptors in global affairs but remain at odds on the question of whether it should be understood as a major security concern⁶⁸. The dissertation seeks to contribute to this field and question by analysing how information challenges have been framed and dealt with in the EU’s case.

Historical studies have analysed information challenges through time, revealing their changing nature as well as the evolving terminology referring to them. Above all, historical perspectives expose the role of religious organisations, political institutions, scholars, corporations, and media organisations in the production of propaganda from Antiquity to modern times⁶⁹. Taylor shares examples dating back to Ancient Greece and refers to cave drawings as “the earliest form of war propaganda”⁷⁰. Scholars have analysed technological breakthroughs, like the printing press and the Internet, as pivotal moments that expanded the scope and reach of mass influence⁷¹. In the West, many eyes are now geared towards Russia and China as major disruptors, but research shows that all great powers have engaged in propaganda. Cull, Culbert, and Welch share a plethora of examples in their *Historical Encyclopaedia*, including from the

⁶³ Lasswell 1971; Lasswell, Lerner, and Speier 1980; Qualter 1962; Taylor 2003; Thomson 1977.

⁶⁴ Antoniadis, Miskimmon, and O’Loughlin 2010; Freedman 2006; Hallahan et al. 2007; Miskimmon, O’Loughlin, and Roselle 2013.

⁶⁵ Nye 2004.

⁶⁶ Bateson 1987; Chong and Druckman 2007; Scheufele 1999.

⁶⁷ Waeber 1995; Buzan, Wæver, and Wilde 1998.

⁶⁸ Gerrits 2018; Lanoszka 2019; Mäklsoo 2018; Miró-Llinares and Aguerri 2023.

⁶⁹ See Cull, Culbert, and Welch 2003; Herman and Chomsky 2002; Kenez 1985; Taylor 2003.

⁷⁰ Taylor 2003, 20.

⁷¹ Eisenstein 2012; MacLeod 2019; Zuboff 2020.

US, Britain, the Catholic Church, as well as Nazi Germany. They explain that the negative connotation attributed to “propaganda” in the post-war era led to the popularisation of “public diplomacy” in the West⁷². In *Active Measures*, Rid analyses Japanese, German, and US influence operations as well as Soviet-era tactics of *dezinformatsiya* which popularised the usage of “disinformation” and led to modern-day Russian information warfare techniques, including hack-and-leak operations, bot networks on social media, and troll factories⁷³.

Simultaneously, the rise of mass communication technologies in the mid-20th century raised questions about their psychological effects and individual susceptibility to misleading information. Scholars in psychology, such as Festinger, examined how individuals deal with cognitive dissonance when confronted with conflicting information, contributing to our understanding of why people accept or reject misinformation⁷⁴. The Elaboration Likelihood Model, developed by Richard Petty and John Cacioppo in the 1980s, furthered this by distinguishing between central and peripheral routes to persuasion⁷⁵. It highlighted the psychological mechanisms behind the spread and acceptance of information, offering insights into how certain messages resonate based on cognitive biases, emotional appeal, and information overload. Psychological research has thus provided a crucial link between individual cognitive processes and the broader socio-political dynamics and implications of misinformation and information warfare.

3.3 Contemporary Perspectives on Information Challenges

In this dissertation, I separate contemporary perspectives from historical ones, identifying the rise of online platforms and social media networks (early 2000s) as an important milestone that significantly impacted the way we understand, study, and respond to information challenges. This section reviews literature that provides insights about contemporary information challenges: (a) the technology they rely on, (b) the reasons why they arise, (c) their socio-political effects, and (d) the responses they warrant.

First, regarding the contemporary technological context, a growing literature looks at the role of online platforms (e.g. social media and search engines) and Artificial Intelligence (AI) in the spread of misinformation and propaganda. Socio-technical research combining insights from social and computer sciences shows that the design of recommender systems—commonly called “algorithms”—has a significant impact on the spread of misinformation because of their engagement-maximising features, which indirectly make false or surprising information go viral because they keep users engaged on the platforms⁷⁶. The design of platforms may also result in the creation of so-called “echo chambers” of like-minded users, fuelling polarisation

⁷² Cull, Culbert, and Welch 2003, 327.

⁷³ Rid 2020.

⁷⁴ Festinger 1957.

⁷⁵ Petty and Cacioppo 1986.

⁷⁶ Bouchaud 2024; Narayanan 2023; Vosoughi, Roy, and Aral 2018.

and amplifying existing bias⁷⁷. Even when presented with cross-ideological information, platforms tend to deepen divides rather than bridge them⁷⁸. Since the popularisation of generative AI, research has increasingly examined the impact of Large Language Models (LLMs) such as ChatGPT on misinformation dynamics. Several studies have shown that AI-generated content is similarly or more persuasive than its human-generated counterparts⁷⁹, making LLMs cheap and effective weapons of information warfare⁸⁰.

Second, a vast literature looks at the contemporary causes of information challenges, which are diverse and multiple, illustrating complex and intertwined causal chains. In addition to the above technological context, social, psychological, and political factors influence the belief in/spread of misinformation online. Socio-psychological factors include cognitive drivers (e.g. lack of analytical thinking, neglect of certain sources) and socio-affective drivers (e.g. in-group attraction, worldviews)⁸¹. These dynamics are particularly visible on social media, where individuals construct their identity and communicate with peers about what they consider to be important or appropriate. Contemporary psychology studies explain that people believe in erroneous information mainly because it supports their existing beliefs and ideology⁸², supporting Welch's claim that "propaganda confirms rather than converts"⁸³. This makes misinformation pervasive and difficult to correct, which psychologists call the Continued Influence Effect⁸⁴.

Political conversations can be polarising, but this dynamic is largely inflated by contemporary technological affordances, i.e. the design of online platforms⁸⁵. As mentioned previously, the recommender systems that rule social media networks and search engines accentuate existing biases and divisions. Additionally, online, people tend to *engage* with misinformation more than accurate information because of the strong emotions it triggers (whether positive or negative): it is often captivating and worthy of sharing/commenting, which increases its reach⁸⁶. This can lead to an overestimation of misinformation's impact. Nevertheless, these dynamics are exploited for advantage, for example by political actors (electoral gains) or by private companies (financial gains), with potentially massive influence when those actors are in positions of power. This leaves marginalised people and minorities particularly at risk of being

⁷⁷ Cinelli et al. 2021; Bessi et al. 2016; Mansoury et al. 2020.

⁷⁸ Barberá et al. 2015.

⁷⁹ Everett, Nurse, and Erola 2016; Huang and Wang 2023; Spitale, Biller-Andorno, and Germani 2023.

⁸⁰ Matz et al. 2024; Goldstein et al. 2024.

⁸¹ Ecker et al. 2022; Faris et al. 2017; Guess, Nagler, and Tucker 2019.

⁸² Roozenbeek et al. 2022.

⁸³ Cull, Culbert, and Welch 2003, xviii.

⁸⁴ Ecker et al. 2022.

⁸⁵ Radicioni et al. 2021.

⁸⁶ Vosoughi, Roy, and Aral 2018; Ecker et al. 2022, 14–15.

manipulated and contributes to systemic inequality, which has been repeatedly shown to hinder both individual opportunities and broader societal prosperity⁸⁷.

Structural factors contributing to information systems are not only social and technological, but also political. Farrell and Newman argue that liberal political institutions, designed to promote openness and cooperation, paradoxically create vulnerabilities that adversaries can exploit⁸⁸. By relying on interconnected information systems, liberal regimes facilitate interference and influence operations, which can be weaponized by authoritarian regimes⁸⁹. Therefore, liberal democracies are particularly vulnerable to information challenges. Still, some experts contend that the bulk of the problem attributed to misinformation and information warfare in liberal democracies resides in ordinary news and betrayals of the public⁹⁰. It raises important ethical and practical questions for liberal regimes, namely, how to balance geostrategic interests and fundamental values of openness and freedom. The dissertation seeks to contribute to this debate by examining critically how a liberal democratic institution, the EU, has responded to information challenges.

With regards to instigators, three culprits stand out from the contemporary literature: private companies, political organisations, and individuals—in other words, everyone. Private actors such as tech companies but also other large corporations benefit financially from the design of addictive smartphones and social media or biased search engines, platforms, and LLMs. Political actors such as politicians, public figures, and international organisations are often responsible for large-scale influence operations, with hopes to impact geostrategic and/or financial interests⁹¹. Recent examples include EU border agency Frontex and Italy’s cover-up of their role in a shipwreck that killed 94 people in the Mediterranean⁹², US Secretary of State Antony Blinken’s dismissal of evidence of Israel’s violations of International Humanitarian Law in his testimony to Congress⁹³, and Russian Ministry of Foreign Affairs’ debunked claim that the missile that hit a children’s hospital in Kyiv was American-made⁹⁴. Lastly, individuals of all kinds share misinformation either knowingly or unknowingly, and with the intention to cause harm or to alert, share, discuss, or debate, based on their ideologies and communication habits. Through network ethnography, Starbird et al. exposed that influence operations and misinformation are inherently collaborative and it is incredibly difficult to distinguish “between orchestrated, explicitly coordinated, information operations and the emergent,

⁸⁷ Dabla-Norris et al. 2015; Deaton 2013; Piketty 2017; Stiglitz 2013.

⁸⁸ Farrell and Newman 2021.

⁸⁹ Bjola and Pamment 2019, 28–43.

⁹⁰ Allen 2023; Wilde 2022.

⁹¹ Woolley and Howard 2019; Bradshaw and Howard 2019.

⁹² Abbas Azimi et al. 2023.

⁹³ Murphy 2024.

⁹⁴ Sheldon et al. 2024.

organic behaviours of an online crowd”⁹⁵. This highlights how crucial the role of individuals is in the development of information challenges.

Third, many studies examine the contemporary effects of misinformation and information warfare on society. Most studies look at their impact on beliefs and online behaviour, but few investigate the effect that they have on offline behaviour⁹⁶. Indeed, it is extremely difficult to measure the real-world impact of information, given the countless factors that influence outcomes and the incredible quantity of data we consume. Data is also sometimes hard to collect, for example from online platforms or government institutions. As pointed out by Bateman et al. in their systematic review, “the research gaps are serious and long-standing”⁹⁷. Still, the literature highlights the systemic troubles misinformation can create in the long term, especially for democratic regimes (which rely on informed, rational public debate): misinformation is correlated with increased epistemic cynicism and selective media consumption⁹⁸. The Continued Influence Effect also indicates long-term effects on memory, reasoning, and decision making⁹⁹, negatively affecting mutually understood notions of truth and reliance on science as a credible method to differentiate facts from fiction. Nevertheless, a growing literature has argued that the reach and impact of misinformation and information warfare are often overestimated¹⁰⁰ or overblown in the pursuit of political interests¹⁰¹. Shapiro and Norton contend that the ambiguity surrounding “misinformation” leads to inconsistent definitions and research methods, complicating the task of understanding how information affects society and leading researchers to adjudicate the truth value of content, in contradiction with scholarly objectivity¹⁰².

Both structural factors (e.g. technology, socio-political context) as well as individual factors (e.g. human psychology, education, habits) influence the creation and development of information challenges, reflecting complex causal chains. They also are highly affected by current events and crises, such as the COVID-19 pandemic or climate change, which foster uncertainty and fear, thereby increasing socio-affective needs (emotional, social connection, and interpersonal support), some of the key drivers of misinformation¹⁰³. Bearing in mind the contemporary context of “polycrisis” and “permacrisis”, i.e. the interconnected and seemingly permanent state of crisis¹⁰⁴, information challenges call for comprehensive frameworks that help understand their broad and multifaceted nature. Some experts have suggested using complexity science and systems thinking to better model and understand convoluted social

⁹⁵ Starbird, Arif, and Wilson 2019, 127:1.

⁹⁶ Murphy et al. 2023.

⁹⁷ Bateman et al. 2021.

⁹⁸ McKay and Tenove 2021; Lewandowsky et al. 2023; Harris, DeMora, and Albarracín 2024.

⁹⁹ Ecker et al. 2022; Lewandowsky et al. 2012.

¹⁰⁰ Fletcher et al. 2018; Guess, Nagler, and Tucker 2019.

¹⁰¹ Camargo and Simon 2022; Belogolova et al. 2024; Wilde 2022.

¹⁰² Shapiro and Norton 2024.

¹⁰³ Ecker et al. 2022; Roozenbeek et al. 2022.

¹⁰⁴ Lawrence et al. 2024; Zatti 2024.

phenomena¹⁰⁵. Koinova et al. suggest embracing “ordered chaos” and the polycentric nature of global governance, focusing on relational aspects rather than the actors themselves¹⁰⁶. Regardless, it seems that the causes and effects of information challenges are far from being well understood.

Fourth, a large part of the literature on misinformation and information warfare explores countermeasures or “interventions” and their effectiveness¹⁰⁷. These can generally be placed in three categories: user-facing solutions, governance, and platform design. User-facing solutions focus on empowering Internet users to analyse digital information critically, with the objective of developing their capacity to detect influence operations and false reports (e.g. critical thinking skills, media literacy, bias awareness, knowledge of common misinformation tactics, fact-checking). Governance focuses on the policy and legal frameworks that affect the digital information space (e.g. cybersecurity, education, transparency requirements, coordination and accountability mechanisms, support for independent media and quality journalism). Platform design focuses on the creation of virtual public spheres that do not incentivise polarisation, hatred, or extremism and instead favour a healthy reflection of public debate (e.g. algorithmic de-amplification, content moderation, redirection, and deplatforming accounts). Building on a review of 223 studies, Courchesne, Ilhardt, and Shapiro explain that most research on the effectiveness of countermeasures focuses on user-facing solutions (especially fact-checking), while much more research is needed to fully understand the impact of information governance and platform interventions¹⁰⁸. Among user-facing responses, repeated pre-bunking has been showed to be more effective in the long term, in comparison to debunking solutions¹⁰⁹.

3.4 The EU’s Approach to Information Challenges

Despite disagreements and shortcomings in the literature about information challenges, policy and legal responses have developed across the globe, mainly at the national and regional levels. The fragmented nature of information governance contrasts with the global character of information challenges, which transcend political borders as communities and ideologies increasingly develop digitally. A few research projects have tracked counter-misinformation measures across the globe, but more up-to-date databases are needed¹¹⁰. Those projects show that, in the US, there is growing pressure to criminalize false electoral information, while states like Texas and California have already enacted regulations enhancing transparency requirements. The federal Foreign Malign Influence Center combats foreign interference, and Section 230 of the Communications Decency Act protects platforms from third-party content

¹⁰⁵ Kwamie et al. 2024; Koliba et al. 2022; Mitchell 2009.

¹⁰⁶ Koinova et al. 2021.

¹⁰⁷ Bjola and Pamment 2019; Courchesne, Ilhardt, and Shapiro 2021; Helmus and Kepe 2021; Kaiser and Mayer 2023; Lewandowsky et al. 2012; van der Linden 2023.

¹⁰⁸ Courchesne, Ilhardt, and Shapiro 2021.

¹⁰⁹ Lewandowsky and van der Linden 2021; Capewell et al. 2024.

¹¹⁰ Funke and Flamini 2019; Lim and Bradshaw 2023; LupaMundi 2024.

liability. In Brazil, spreading misinformation during elections can lead to penalties, including fines or imprisonment, as per the recent “Fake News Law”. In China, Article 12 of the 2016 Cybersecurity Law states that no individual or organization should use the Internet to create or disseminate false information that disrupts economic and social order. The UK also has laws against sharing false information, with the Malicious Communications Act imposing up to two years in prison. The Online Safety Bill, approved in 2023, obliges internet companies to remove illegal content and established an Advisory Committee.¹¹¹

In the EU, national counter-misinformation measures have developed slowly, with the exception of the Baltic states, which have been at the forefront of strategic communication policies and particularly sensitive to pro-Kremlin propaganda given their proximity to Russia and their significant Russophone population: about 45% in Riga (Latvia), 43% in Tallinn (Estonia), and 20% in Vilnius (Lithuania), but up to 95% in certain towns¹¹². Figure 1 below represent the proportions of native Russian speakers and ethnic Russians. In the mid-2010s, the Baltic states thus swiftly reacted to heightening tensions with Russia and its increasing reliance on information warfare, by restricting broadcasting that incited hatred¹¹³.

Figure 1: Maps of native Russian speakers and ethnic Russians in the Baltic states, 2014¹¹⁴



Sources: The Economist, 2014; Stratfor, 2014.

¹¹¹ LupaMundi 2024.

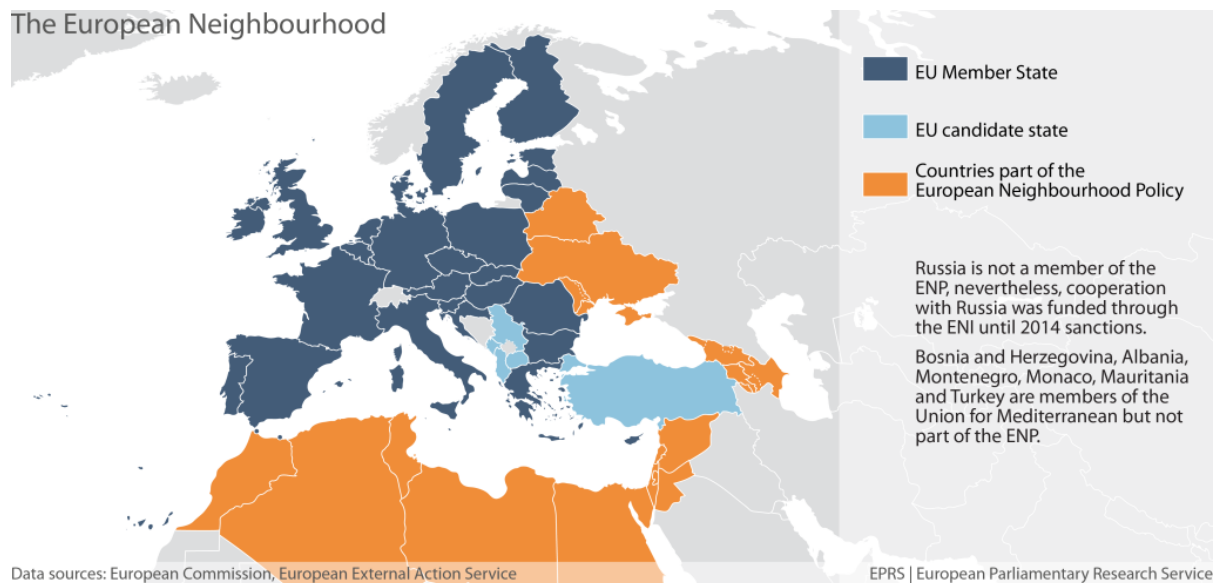
¹¹² Simonyan 2022, 146.

¹¹³ Vilson 2016.

¹¹⁴ The Economist 2014; Stratfor 2014.

The escalating tensions between the EU and Russia are rooted in a complex interplay of geopolitical factors. In 2004, the EU enlarged eastward (Czechia, Cyprus, Estonia, Latvia, Lithuania, Hungary, Malta, Poland, Slovenia, and Slovakia) and launched the European Neighbourhood Policy (ENP) with bordering countries, illustrated in Figure 2. Russia perceived it as a direct threat to its sphere of influence and declined to join, instead establishing the “Common Spaces” for cooperation in 2003, explain Wiegand and Schulz¹¹⁵. In 2008, the Bucharest NATO summit mentioned potential future membership of Georgia and Ukraine. A few months later, the Russo-Georgian war marked a significant rise in tensions, demonstrating Russia's willingness to use military force after Georgia attempted to reassert control over the region of South Ossetia, the site of violence and tensions for years. In 2009, the EU launched the Eastern Partnership (EaP) policy, specifically focused on Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine. The 2013-14 crisis in Ukraine, marked by Russia's illegal annexation of Crimea and support for separatists in eastern Ukraine, further deepened the rift between the EU and Russia. This event was seen by many as a direct challenge to the post-Cold War European security order¹¹⁶. The 2022 invasion of Ukraine, a full-scale military conflict with devastating consequences, represents the most significant escalation in EU-Russia tensions since the Cold War.

Figure 2: Map of EU Member States, candidate countries, and European Neighbourhood Policy¹¹⁷



Source: EPRS, 2016

¹¹⁵ Wiegand and Schulz 2015.

¹¹⁶ Menon and Rumer 2015; Mäklsoo 2019; Averde 2016.

¹¹⁷ EPRS 2016.

Scholars have offered diverse perspectives on this escalation of tensions, highlighting the nuanced geopolitical context in which EU counter-misinformation measures emerged. This is essential to understand perceptions of insecurity in the EU as well as key areas of contestation that feed misinformation and influence operations on the European continent. While most condemned Russia's violations of International Law, many also acknowledged mistakes from the West. Mearsheimer argues that the EU's eastward expansion and NATO's enlargement were key factors in provoking Russia's aggressive behaviour, driven by a desire to maintain its security and prevent the encroachment of Western institutions¹¹⁸. MacFarlane and Menon similarly argue that "Europeans were negligent in their failure to take seriously transparent and long-standing Russian positions on the shared neighbourhood"¹¹⁹. Garton Ash contends that the West made a fundamental mistake by thinking that Russia would give up ex-Soviet territories so easily, but that it is naïve to think that Ukraine would have peacefully existed without prospects of NATO membership, and it does not justify war¹²⁰.

Joint EU measures against misinformation and information warfare emerged promptly after the 2013-14 Ukraine crisis, starting with the creation of the East StratCom Task Force (ESTF). Progressively, the EU policy toolkit expanded, including in strategic communication, media literacy, media pluralism, transparency requirements, and content moderation, of which the key milestones are listed in Figure 3 below (see [Annex G](#) for a wider overview). During the COVID-19 pandemic, the EU encountered information challenges stemming from misinformation and geopolitical competition exemplified by mask and vaccine diplomacy¹²¹. Faced with the limited impact of its non-binding measures, the EU prepared the ground for the far-reaching Digital Services Act, proposed in December 2020 and adopted in September 2022. Following Russia's invasion of Ukraine in February 2022, the EU adopted new restrictive measures to halt the spread of misinformation including a broadcasting ban on Russian state-sponsored media, which has grown to count eighteen media outlets at the time of writing¹²².

¹¹⁸ Mearsheimer 2014.

¹¹⁹ MacFarlane and Menon 2014, 100.

¹²⁰ The War in Ukraine and the Future of Democracy in Central Europe 2022.

¹²¹ Juncos 2021; Leigh 2020; Hosa, Kelmendi, and Popescu 2021.

¹²² EU sanctions against Russia 2024.

Figure 3: Key Developments in the EU Counter-Misinformation Toolkit—author’s graph¹²³



The literature analysing the development of EU counter-misinformation policies is broad. This section focuses on three milestones standing out from this scholarship: the creation of the ESTF in 2015, the EU’s response to the COVID-19 “infodemic”, and the ban on Russian state-sponsored media, starting with *RT* and *Sputnik* in 2022.

First, on the creation of the ESTF, Vilson shows that it reflects the Europeanization of foreign and security policy and the expansion of EU competences in the field of strategic communication¹²⁴. Wagnsson and Hellman argue that the work of the ESTF and the development of joint counter-disinformation policies has led the EU to lose reflexivity and normative power¹²⁵. They contend that the EU must avoid presenting others as existential threats or inferior in order not to damage its soft power globally. Hedling adds to the literature on the ESTF by showing that it transformed the practice of diplomacy within the EEAS, which

¹²³ These documents were selected based on their direct impact on misinformation/disinformation issues.

¹²⁴ Vilson 2016.

¹²⁵ Wagnsson and Hellman 2018.

not only aimed its public diplomacy at foreign publics but also domestic ones¹²⁶. What remains unclear are the deliberate acts and underlying dynamics which allowed for the unit to emerge and make such a long-standing impact on the EU's approach to information challenges.

Second, on the EU's response to the COVID-19 "infodemic", Harrison explains that the measures in place at the time of the pandemic outbreak—policy guidelines and a voluntary code of practice—were insufficient to meaningfully respond to the challenge¹²⁷. He argues that this hands-off approach was however adapted to the complexity of the situation:

(...) the delicate balancing act between promoting free forums of public debate and tackling the disinformation which pollutes these forums makes the cautious nature of the initial steps by the Commission understandable. Furthermore, from a fundamental rights perspective, it would have been far worse if the Commission had presented a fixed solution to such an evolving problem as disinformation.¹²⁸

Nevertheless, the shortcoming exposed during the pandemic gave the impetus for more forceful and binding measures such as the Digital Services Act. The EU's management of the COVID-19 pandemic has been the subject of vast scholarly study highlighting the legitimacy gaps and democratic deficits that resulted from a lack of transparent decision-making and public debate, as well as the disconnect between the EU's pragmatic response and its fundamental values¹²⁹. Wolff and Ladi argue that the pandemic raised questions about sovereignty, solidarity, and public trust within the EU, leading to a re-evaluation of emergency governance practices¹³⁰. More broadly, scholars agree that the normalisation of "emergency politics" in the EU undermines its democratic legitimacy and long-term strategic planning¹³¹. This dissertation seeks to deepen our understanding of EU emergency politics in the field of information governance by revealing the actors, policy-making structures, and broader dynamics that enable it.

Third, the ban of Russian state-sponsored media adopted in 2022 is an instructive example of emergency measures in information governance and one that highlights important tensions between security and freedom of speech. The literature has been critical in three ways. First, experts have questioned the proportionality of the measure, given its broad restrictions on freedom of speech and of the media¹³². Second, scholars have claimed that the Council did not have the legal capacity to regulate the media space, a shared competence allowing both the EU and member states to legislate, provided that the EU does not overstep its boundaries in matters

¹²⁶ Hedling 2021.

¹²⁷ Harrison 2021.

¹²⁸ Ibid., 23–24.

¹²⁹ Boin and Rhinard 2023; Kreuder-Sonnen and White 2022.

¹³⁰ Wolff and Ladi 2020.

¹³¹ Rhinard 2019; Schmidt 2022.

¹³² Mendiratta and Alkiviadou 2022; Ó Fathaigh and Voorhoof 2022.

of cultural and media diversity¹³³. Lastly, criticism came from the limited effectiveness and implementation of the ban, which ultimately further divides the European information space¹³⁴. Once again, the underlying dynamics that allowed for this measure to emerge are unclear, which limits scholarly understanding of information challenges' nature.

More generally, European and diplomatic studies scholars have indicated that EU counter-misinformation policies show overlapping and potentially conflicting security-related values (coherence and efficiency vs. independent democratic judgement) as well as opposing logics (securitisation vs self-regulation), undermining its credibility on the world stage¹³⁵. Mälksoo notably argues that hybrid warfare, including information warfare, is a manifestation of ontological insecurity, i.e. challenges to “the actor’s ability to act in the world with basic confidence about how the world works and her own place within it”¹³⁶. She views the recent developments in EU information governance as attempts to preserve their organisational security and thus as nothing more than political games presented as existential threats. This is particularly important given that some EU counter-misinformation measures have emerged from procedures with reduced democratic oversight (e.g. as part of the CFSP), which may decrease perceptions of their legitimacy. As explained by crisis management scholars Boin and Rhinard: “(...) the honeymoon effect is short-lived and the emergence of competing crisis frames is pretty much guaranteed. Accusations of ‘backroom decision-making’ are never far away.”¹³⁷. Furthermore, recent studies indicate that the European Commission increasingly shapes the agenda on information challenges¹³⁸, which raises further questions about the interests that EU counter-misinformation policies protect. The democratic deficit that this institution suffers from has long been a central topic of debate in European studies¹³⁹, thus its policies governing information led to criticism from free speech advocates¹⁴⁰.

Ultimately, it will be crucial for both scholars and policymakers to address the fundamental debates surrounding counter-misinformation policies, namely, regarding the nature of the threat they seek to address, their legitimacy, and the delicate balancing act they perform between political strategic interests and the liberal democratic values that the EU rests upon. More generally, crises are known to impact European integration in different ways and research shows that policymaking dynamics and perceptions of their legitimacy are core determinants¹⁴¹. The limited transparency and accountability mechanisms of international organisations, insufficient public engagement, and information asymmetries that favour elite

¹³³ Kaye 2022; Popović 2022.

¹³⁴ Hoyle and Pijpers 2022; Allen 2023.

¹³⁵ Ördén 2019; Casero-Ripollés, Tuñón, and Bouza-García 2023; Bjola and Pamment 2019, 66–80.

¹³⁶ Mälksoo 2018, 375.

¹³⁷ Boin and Rhinard 2023, 662.

¹³⁸ Datzler and Lonardo 2023; Ördén 2019; Saurwein and Spencer-Smith 2020.

¹³⁹ Norris 1997; Follesdal and Hix 2006.

¹⁴⁰ Mchangama 2023.

¹⁴¹ Börzel 2023; Ferrara and Kriesi 2022; Jones, Kelemen, and Meunier 2016; Schimmelfennig 2018; Schmidt 2013.

viewpoints contribute to perceptions of illegitimacy, which negatively impact joint governance mechanisms¹⁴². Schmidt notably conceptualised “throughput legitimacy”—efficacy, accountability, transparency, openness and inclusiveness of policymaking processes—as an essential yet neglected dimension to foster greater public trust in EU institutions and address democratic deficits¹⁴³. Noting the rise of Euroscepticism, especially in times of crisis¹⁴⁴, this challenge is of paramount importance for the EU and a central concern for the academic community. Hooghe and Marks have argued that while European integration once benefited from “permissive consensus” (where public support allowed elites to pursue integration), it now faces “constraining dissensus”, meaning that citizens increasingly challenge and constrain integration processes¹⁴⁵. This shift has created polarized opinions on integration, with identity politics playing a central role. Hooghe and Marks contend that as integration deepens, it provokes more public debate, causing conflicts rooted in national identity, which leads to fragmentation in EU support and broader Euroscepticism among Member States¹⁴⁶.

European studies scholars have argued that regional security governance, which has been the cradle of counter-misinformation policies, is particularly vulnerable to these dynamics. Foreign and security policy has traditionally remained outside of public consultation because it is central to a state's sovereignty, i.e. its autonomy and control over its territory, resources, and citizens. In the EU, this understanding means that the CFSP has remained (in theory) an intergovernmental exercise, with EU member states reluctant to cede authority to supranational institutions. Yet, several scholars have found that the CFSP relies on policymaking structures that go beyond intergovernmentalism, with untransparent and consensus-seeking practices that further restrict democratic oversight and negatively affect the perceived legitimacy of EU foreign and security policy¹⁴⁷. Building on a communicative perspective on European security that focuses on citizens' rights rather states' sovereignty, Sjursen suggests that “it would make sense to talk about deliberation and actors seeking agreement through arguments also in the issue area of European security”¹⁴⁸. This dissertation seeks to contribute to this scholarly debate by unpacking the processes from which counter-misinformation policies have emerged in the EU, not only to enhance our scholarly understanding of information challenges, but also to deepen our knowledge of security policymaking in the EU and its consequences on legitimacy.

¹⁴² Dellmuth et al. 2022.

¹⁴³ Schmidt 2013.

¹⁴⁴ Pirro and Taggart 2018; Torreblanca and Leonard 2013.

¹⁴⁵ Hooghe and Marks 2009.

¹⁴⁶ Ibid.

¹⁴⁷ Juncos and Reynolds 2007; Maurer and Wright 2021; Sjursen 2011.

¹⁴⁸ Sjursen 2004, 123.

3.5 Summary

This literature review has offered a comprehensive review of the state of research helpful to answer the central questions of this dissertation, i.e. *why EU counter-misinformation policies emerged the way they did, how they have evolved, and which lessons we can draw from this case study about information governance*. The literature is vast and far-reaching, with a myriad of perspectives helping to make sense of information challenges and their governance. International Relations, communication, historical, and diplomatic studies bring clarity to the systemic structures and practices that influence the production and propagation of information. Psychology informs us about the individual factors that lead to erroneous beliefs and the feedback loops that reinforce them. Computer science explains the technical aspects that shape information production, propagation, and consumption, often accentuating the abovementioned dynamics. Together, these fields help to better grasp the challenges at hand and the solutions that may address them, as further exposed in this thesis. To make sense of the EU's approach, the European studies literature is rich in theories and empirical research. In particular, scholarly work on emergency politics, foreign and security policymaking, integration, and legitimacy helps to identify the debates to which this dissertation contributes and the broader trends in European politics that it helps capture. Three preliminary conclusions stand out from this literature review.

First, information challenges are often misunderstood and have been conceptualised in ways that are biased and do not facilitate global governance despite their transboundary nature. In an attempt to address these shortcomings, [Part I](#) of this dissertation provides simple definitions of misinformation, disinformation, propaganda, strategic communication, public diplomacy, framing, strategic narratives, and soft power—central to study counter-misinformation policies. It also compares them with influence operations, psychological operations, and hybrid threats. [Part II](#) delves into the political background of contemporary understandings of misinformation, with an in-depth study of the EU case that reveals how political interests influence how information challenges are framed and responded to. Building on the analysis of the EU case, [Part III](#) proposes a novel conceptualisation of information as complex networked systems. It seeks to provide new, useful ways of theorising information challenges and their governance, with a focus on facilitating international cooperation and mutual understanding.

Second, how we understand and study information challenges is tightly connected to political discourse and policy responses. To unpack these dynamics from a contemporary perspective, this dissertation looks at the case of EU counter-misinformation policies, which are far-reaching both in their development and impact. [Part II](#) of this dissertation examines the EU's approach through three major crises: Russia's illegal annexation of Crimea in 2014, the COVID-19 pandemic outbreak of 2020, and the Russian invasion of Ukraine in 2022. Looking at the information challenges that these crises produced, the dissertation reveals the causal factors and mechanisms, especially the political dynamics, that have influenced European understandings and responses. It contributes to debates surrounding the legitimacy of such measures and their place within governance structures. Each chapter in Section II deepens our understanding of the interests and logics that drive political actors when developing counter-

misinformation policies. [Chapter 2](#) shows the influence of the Baltic states as early advocates of joint countermeasures, following heightened tensions between the EU and Russia. It refines our understanding of small states' influence in EU policymaking. [Chapter 3](#) examines the interplay of internal and external information challenges related to the COVID-19 pandemic and the EU's unpreparedness to deal with them, which laid the ground for more forceful tools. [Chapter 4](#) shows how the securitisation of information challenges (i.e. their framing as existential security threats) was a fundamental factor in the development of the EU's approach, resulting in increasingly restrictive measures that have drawn criticism and showcased important contradictions in EU governance. It refines collective securitisation theory by clarifying how the recursive interactions between EU institutions and Member States take place and what they need to make securitisation legitimate.

Third, much is still unknown about EU counter-misinformation policymaking, as processes are untransparent and increasingly happening in contexts of emergency, with special procedures that further complicate democratic oversight. As explained by Bouza García and Oleart:

There is a wide literature on the phenomenon of disinformation and 'fake news', but we know relatively little about the specific ways in which different actors compete at the level of EU public policy to regulate it, as well as its normative implications.¹⁴⁹

To contribute to the production of empirical knowledge in this field, this dissertation unpacks two processes in detail: the creation of the ESTF in 2015 ([Chapter 2](#)) and the adoption of the broadcasting ban on Russian state-sponsored media *RT* and *Sputnik* in 2022 ([Chapter 4](#)). The dissertation identifies key players, the strategies they employed to get their interests across, and the procedures used to lead proposals to fruition. Rather than evaluating the appropriateness of such processes, it intends to elucidate their functioning in an attempt to contribute to a deeper understanding of EU foreign and security policymaking as well as EU politics more broadly. It critically assesses such processes considering legal and ethical norms characteristic of the EU and shared with other liberal democratic regimes, with the objective of identifying practical lessons learned from this case.

¹⁴⁹ Bouza García and Oleart 2023, 2.

4. Research Design

4.1 Research Questions

Building on the literature on information challenges, this dissertation explores the origins, evolution, and prospects of counter-misinformation policies in the EU. Specifically, it seeks to unveil the socio-political process that led to their emergence and development over the last decade (2014-2024), as well as the lessons that this highlights, by asking:

- A. Why did counter-misinformation policies emerge the way they did in the EU?
- B. How have EU counter-misinformation policies evolved since their inception?
- C. What does the EU case teach us about information governance in general?

Despite an originally divided political context on the Ukraine question, counter-misinformation policies and broader information governance developed at the EU level in the aftermath of the 2013-14 Ukraine crisis, first as a matter of the CFSP and as a unit countering pro-Kremlin propaganda within the EEAS. Since then, information governance seems to have pervaded many more policy areas, such as digital policy (e.g. online platforms regulations, data protection), social policy (e.g. media literacy, public health campaigns), and media policy (e.g. support for journalists, broadcasting bans), with measures that are increasingly binding and restrictive. The thesis does not aim to compare or assess the appropriateness of such policy outcomes, its primary objective is to retrace the key causal mechanisms that characterise EU information governance, from its emergence to its latest developments.

By asking those central questions, the thesis addresses bigger conceptual, ethical, and normative questions faced by other global actors, including:

- How do modern understandings of information challenges help address them?
- How do contemporary policies align with liberal democratic values?
- How can policies be optimised for public good?

These questions contribute to a broader and deeper knowledge about information challenges and their governance. Information challenges transcend borders; it is therefore important to consider global, universal perspectives. The EU is known for its highly developed and detailed policy and legal framework; hence it offers a great case study to assess wider theories about information challenges and their governance (most likely case¹⁵⁰). If the theory does not hold in this well-suited context, its broader relevance is questioned, though success in the EU case does not necessarily ensure its wider applicability. The dissertation does not aim to generalise all findings beyond the case of the EU (some of them are inherently linked to its policymaking procedures). However, its secondary objective is to derive general insights about information governance.

¹⁵⁰ See related interview techniques: Mosley 2013, 19.

The gaps that those questions and objectives seek to address are twofold. First, from an empirical perspective, this within-case analysis contributes to a more detailed understanding of European policies related to misinformation and information warfare, as well as the process that led to their creation. It provides a comprehensive analysis of information governance in the EU, revealing the complex causal mechanisms behind its evolution. In Section II, the thesis unpacks three milestones in the development of EU counter-misinformation measures: (1) Russia's illegal annexation of Crimea and the subsequent creation of the East StratCom Task Force, (2) the COVID-19 pandemic outbreak and the subsequent strengthening of EU response mechanisms, and (3) Russia's invasion of Ukraine and the EU's subsequent broadcasting ban on Russian state-sponsored media *RT* and *Sputnik*. It deconstructs those responses in detail, showing the dynamics and actors that led to their adoption and the challenges encountered along the way. The influence of the Baltic states and the collective securitisation of information challenges stand out as major factors to explain why the EU responded the way that it did after the escalation of tensions between Russia and the EU.

Second, from a theoretical perspective, the thesis contributes to a deeper understanding of information challenges, their ontology, and their governance in the EU, with implications for scholarly studies on security and digital policy more broadly. Section I defines key concepts and critically analyses their usefulness for understanding and addressing information challenges. It shows that inter-disciplinary approaches (integrating theories, methods, and insights from different academic fields) are crucial. Many dynamics are still unclear and studies have concentrated on Western worldviews, hindering global cooperation to address those challenges. Section II unpacks how information challenges have been conceptualised and responded to at the EU level. By studying the processes that led to new EU counter-misinformation measures, the thesis critically assesses the nature of the problem they are designed to tackle, as well as some of the theories that explain EU policymaking in this field. Those endeavours contribute to ongoing scholarly debates about the usefulness of misinformation studies, the effectiveness and legitimacy of counter-misinformation measures, balancing geopolitical interests with fundamental freedoms, as well as differentiating between politics and security when dealing with information challenges. No single theory or approach seems to fully explain the development of information governance in the EU, nor to provide a holistic framework for meaningful solutions. Therefore, in Section III, the thesis builds the foundation of a novel theoretical understanding of information challenges and their governance, making sense of the seemingly chaotic nature of the problem and providing avenues for transboundary mutual understanding.

Figure 4: Overview of Research Questions and Contributions

Research Questions	Empirical Contribution	Theoretical Contribution	Chapters
(A) <i>Why did counter-misinformation policies emerge the way they did in the EU?</i>	• EU foreign and security policymaking dynamics in information governance • Origins of EU counter-misinformation policies	• Small state influence in the EU • Ontology of contemporary information challenges and governance in the EU	Chapter 2

	• Creation of the East StratCom Task Force		
<i>(B) How have EU counter-misinformation policies evolved since their inception?</i>	• EU foreign and security policymaking dynamics in information governance • Expansion of EU counter-misinformation policies • EU response to “infodemic” • Adoption of the EU’s ban on RT and Sputnik	• Collective securitisation theory • Ontology of contemporary information challenges and governance in the EU	Chapter 3 Chapter 4
<i>(C) What does the EU case teach us about information governance in general?</i>	• EU approach to information challenges and governance • Ethical and practical challenges for liberal democracies and global governance	• Complexity science • Ontology of contemporary information challenges • Global information governance	Chapter 1 Chapter 5

4.2 Methodology

In addressing these research questions, the dissertation deconstructs three key outcomes of interest in EU the development of information governance:

- (1) the creation of the East StratCom Task Force (ESTF) in 2015 (the first counter-misinformation policy adopted at the EU level)
- (2) the EU’s response to information challenges related to the COVID-19 pandemic outbreak in 2020 (reflecting a hands-off approach with non-binding measures)
- (3) the adoption of restrictive measures against Russian state-sponsored media in 2022 (the most stringent counter-misinformation measure adopted at the EU level)

In Section II, each chapter provides detailed accounts of why and how those developments happened. It informs the reader about their socio-political background and important drivers such as: contextual crises, external disruptions, dynamics between EU institutions and Member States, techniques to influence EU policymaking, crisis decision-making procedures, and financial instruments available for novel policy tools. The analysis not only deepens our understanding of EU foreign and security policymaking dynamics in relation to information governance, but also contributes to scholarly debates about the legitimacy of such measures (and thus their acceptance or contestation) and their place within governance structures (e.g. as foreign and security issues). In Section I and Section III, the dissertation reflects on what this analysis teaches us about information challenges and their governance, not only at the EU level but also at the global level, with implications for both the practice and study of information governance.

Information challenges and their governance involve a multiplicity of explanatory factors, both endogenous and exogenous, with complex causal effects unfolding over time. In this case, Hall explains that outcomes depend on an intricate set of causal mechanisms that cannot be reduced

to a strictly defined independent variables¹⁵¹. The explanatory factors are necessary but not sufficient on their own. It builds on a counterfactual approach to causation¹⁵² that draws inference from necessary conditions and the explanation of individual events, often through qualitative methods. Necessary conditions directly imply a key counterfactual (i.e. the event not happening) and fit in multivariate explanations. In *Explaining War and Peace*, Goertz and Levy identify four characteristics for this type of conceptual framework, which they call “powder keg”:

- The explanatory model is conjunctural. Necessary condition hypotheses virtually always imply conjunctural theories.
- The model is very nonlinear since the outcome is not the sum of the individual effects.
- The process is often contingent in nature: only when the necessary conditions happen to be present together does the outcome occur.
- Most applications of this model have two kinds of variables: (1) structural, background, contextual and (2) catalysts such as individual agency, decisions, events.¹⁵³

These points help to organise and specify the hypothesized explanatory factors in the complex causal chains underpinning the development of EU information governance.

Therefore, based on the “powder keg” model as well as the literature review and preliminary analysis of the EU case, the thesis hypothesizes a **multi-causal explanation** to make sense of the emergence and development of EU information governance that can be reduced as follows:

- a) **a volatile context**, created by the heightening tensions between the EU and Russia and the unruly nature of the Internet;
- b) **legal and political norms**, such as decision-making procedures in EU foreign policy and coalition of like-minded states in Europe;
- c) **exogenous shocks incentivising policy development**, for instance the 2013-14 Ukraine crisis, the COVID-19 pandemic, and the 2022 Russian invasion of Ukraine;
- d) **endogenous stimuli acting as catalysts for new policies**, for instance the Baltic states being particularly vocal about the need for stronger EU strategic communication.

Should this hypothesized multi-causal explanation be correct, empirical data should confirm that those factors *jointly* led to the emergence and development of EU counter-misinformation as described above, i.e. a foreign and security policy enacted as part of a crisis response in a volatile political and technological context, which progressively grew in scope and nature because of repeated endogenous and exogenous stimuli boosting the perceived necessity and appropriateness of such policies. Alternatives to this hypothesis would demonstrate that any of those factors was not necessary for the emergence and development of EU counter-

¹⁵¹ Hall 2003.

¹⁵² Lewis 1986.

¹⁵³ Goertz and Levy 2007, 38–39.

misinformation policies, hence showing that it would have happened regardless, or that one of those factors takes precedence in terms of its explanatory power, showing that it happened solely because of it.

To test and refine those hypotheses, the research project used a methodology inspired by process-tracing and rooted in the qualitative analysis of multiple types of data examined in triangulation to compensate for gaps and biases. This approach fits the abovementioned guidance of Hall, Lewis, Goertz, and Levy when analysing progressive complex causal effects¹⁵⁴. According to Beach and Pedersen, process-tracing is “an iterative research strategy that aims to trace the complex conglomerate of systematic and case-specific causal mechanisms that produced the outcome in question”¹⁵⁵. Process-tracing originated in cognitive psychology, where it was developed to study decision-making and problem-solving by analysing the sequence of thought processes¹⁵⁶. Researchers used it to investigate how individuals interpret information and arrive at conclusions. By the 1980s, the method was adapted in political science by scholars like George and Bennett as a form of within-case analysis¹⁵⁷. Its systematic approach to analysing causal steps allowed for a more nuanced understanding of complex social and political phenomena, making it an invaluable tool for exploring context-specific causal inference in qualitative research. With this methodology, interviews can be used “to construct analytic narratives to reveal the underlying rational choice games that structure incentives and produce action”¹⁵⁸.

In this thesis, process-tracing is used as a guiding logic, in the sense that its core principles are used to identify key causal factors by affirming their explanatory power without performing strict process-tracing tests for causal inference¹⁵⁹. It accommodates the research objectives in three ways. First, it allows delving into the process with a depth that would not be available with quantitative methods. Second, it focuses on invested actors, their logic of interaction, and how they aggregate to produce a collective outcome, which are crucial elements when analysing complex EU policymaking processes. Finally, it helps identifying necessary conditions and understanding how they conjunct in a causal chain of events. This fits my aim to better grasp the development of EU counter-misinformation policies and its implications for our understanding of information challenges and their governance, as opposed to identifying one unique or strongest causal factor, which is not part of this dissertation’s objectives. This approach has several disadvantages, such as the risk of selection bias when choosing cases or evidence, which can threaten external validity and generalizability. It is also time-intensive and may suffer from confirmation bias if ambiguous evidence is interpreted to fit pre-existing theories. Despite these limitations, process-tracing remains a valuable tool for causal analysis if

¹⁵⁴ Hall 2003; Lewis 1986; Goertz and Levy 2007.

¹⁵⁵ Beach and Pedersen 2019, 19.

¹⁵⁶ Bennett and Checkel 2014, 5.

¹⁵⁷ Collier 2011, 823.

¹⁵⁸ Mosley 2013, 118.

¹⁵⁹ See Bennett and Checkel 2014, 136–130; Mosley 2013, 40.

based on clear hypotheses and scope conditions¹⁶⁰, which is why this dissertation establishes them in this section. The research project clarified its initial hypothesis and the empirical tests that would prove or disprove it, identified causal mechanisms derived *ex ante* from theoretical and empirical considerations, focused on crucially puzzling developments, and explained clearly the broader conceptual, normative, and ethical questions it sought to address.

4.3 Empirical Data and its Organisation

The empirical data used in this dissertation includes **50 interviews** with policymakers, civil society organisations, and experts, as well as legal texts such as EU regulations and directives, policy documents, including action plans and non-papers, voting records, speeches, press releases, think tank publications, and news media reports—all analysed in triangulation to offset gaps and biases. Documents were obtained on the EU’s official websites, either through the public registers of EU institutions or by means of a request to their General Secretariat. In total, **above 400 documents** were consulted and/or analysed.

The Appendix lists interviews, codebooks, example interview information sheet, template participation consent form, and the key policy and legal documents examined. Mosley’s mixed-methods, multilevel research design described in *Interview Research in Political Science* was used as a comprehensive guide to prepare, conduct, and analyse interviews’ content¹⁶¹. It provides detailed guidance on designing interview-based studies, sampling, questioning techniques, and data analysis, with attention to ethics and practical challenges. Through case studies, it also demonstrates how interviews can enrich our understanding of political processes, behaviours, and institutional dynamics across diverse contexts.

Sampling: Interviews were conducted between 2019 and 2024, in majority in Brussels, but also in The Hague, London, Oslo, and online. Interviewees were invited to participate anonymously based on their role in or knowledge of the policy processes under scrutiny. Building on Mosleys’ sampling strategy¹⁶², preliminary research was conducted to identify relevant procedures and meeting formats, from which relevant individuals were identified using the European Commission website’s organigrammes and official directory. For example, to unpack the creation of the ESTF in 2015, I searched for relevant policy documents on the EU Council website (e.g. meeting minutes, action plan, council conclusions) searching for the keywords “East StratCom Task Force” and “Strategic Communication”, which allowed to sketch a rough timeline and identify preliminary sites of discussions. I interviewed members of the team who further informed me about where and when the policy development was discussed in the Council. I then identified individuals from Permanent Representations in the relevant Council configurations and working groups, including COREPER II, PSC, and COEST. Individuals working within the European Commission and the EEAS were also

¹⁶⁰ Bennett and Checkel 2014, 10–31; Collier 2011, 825.

¹⁶¹ Mosley 2013.

¹⁶² Ibid., 31–36.

interviewed, as well as experts knowledgeable about the policy development but not directly involved in it, for example within the EU Institute for Security Studies and European Endowment for Democracy. From these, I obtained further interviews (snowballing technique) as well as confidential data and non-public documents such as the 2015 non-paper of the Foreign Ministers of Denmark, Estonia, Lithuania, and the UK that suggested a series of measures to boost the EU's response to pro-Kremlin propaganda.

Data Management: All interviewees received an information sheet that detailed the purpose of the research project, the conditions of their participation, how data will be used and stored, and where they can raise concerns, of which an example is available in the appendix. All interviewees filled and signed a participation consent form, of which a template is available in the appendix. These efforts to make the interview and broader research project safe and transparent helped create mutual trust with interviewees, who seemed most of the time happy to share their experience with the guarantee of anonymity, offered to every participant. For this reason, particular caution has been exercised to not allow their identification.

Treatment: All interviews were semi-structured and lasted between 30 and 120 minutes. Guiding questions revolved around the identification of the policymaking processes' key causal factors, actors, opportunities, and challenges. Interviewees were asked to introduce themselves, their work, and their relation to the development under scrutiny. Then, interviewees were asked more specific questions about the policymaking process depending on their role, for instance "What do you know about the process that led to this measure?", "Who was the most supportive and the least supportive of this measure being adopted?", and "What were their priorities?". In addition, interviewees were asked to share about their perceptions surrounding information challenges and their governance (e.g. legitimacy, effectiveness, ethical value), to better grasp how they are socially constructed in EU policymaking circles. Information was constantly checked against other sources from different interest groups to test the strength of the causal inference, even in small-N designs with non-random samples¹⁶³.

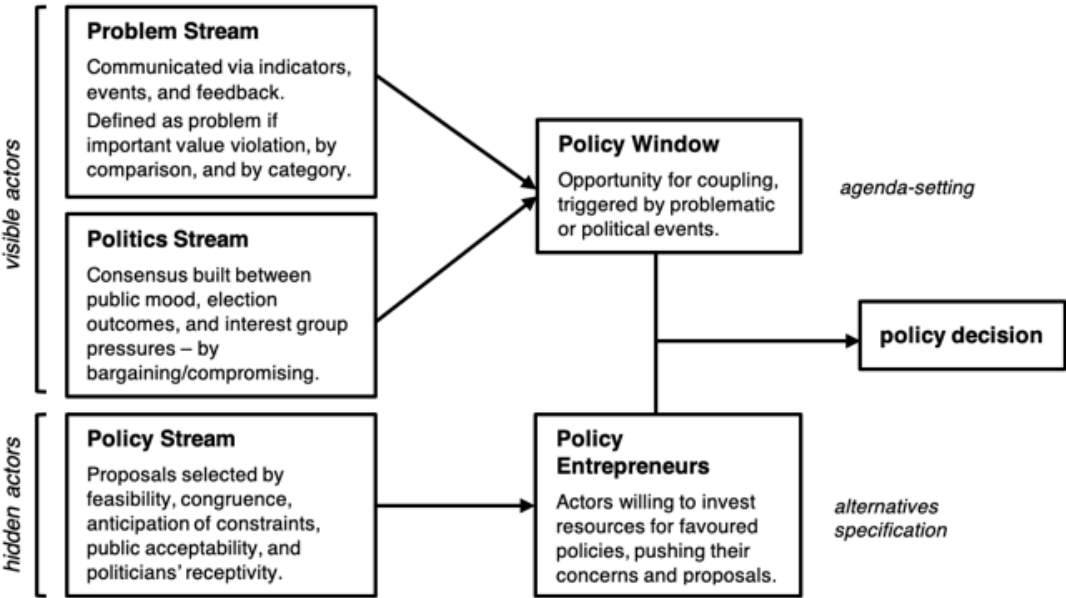
Analysis: Most interviews were recorded, transcribed, and analysed with document analysis software NVivo and Atlas.ti (47 out of 50). These software help organising, coding, and identifying patterns, themes, and relationships in text files, such as word frequency. All interview transcripts were coded based on key questions and themes identified during the preliminary analysis and adjusted as subjects came up during conversations. The codebooks resulting from those document analyses is available in the appendix. They were useful to identify and compare the explanatory power of evidence, as per the methodology outlined above, and perform informal process-tracing tests that test the validity and strength of the arguments made in this dissertation.

¹⁶³ Collier 2011, 824.

Conceptual Framework: To organise and analyse the data, the research project used the Multiple Stream Model (MSM)¹⁶⁴, based on the “garbage can” model of organizational choice¹⁶⁵. This conceptual framework explains policy outcomes by analysing pre-decision processes. It has been widely used in public policy literature and applied across diverse contexts, including the EU¹⁶⁶. Kingdon identifies three streams—problems, politics, and policy—which evolve separately until a “window of opportunity” arises, allowing them to converge (see Figure 5). This triggers policy decisions, facilitated by “policy entrepreneurs” who capitalize on favourable conditions.

Kingdon's SMS provides a valuable analytical tool for understanding EU policymaking and its complex institutional structure. By examining the convergence of problem, policy, and political streams, we can identify the critical junctures and windows of opportunity that shape the EU's policy agenda. The MSM helps clarify how each institution’s priorities and agendas influence the convergence of interests and ideas in political cycles. It also helps capture the way national interests concur in the Council, where Member States defend their own views and priorities, opening “windows of opportunities” when they align. The MSM’s idea of a policy window is especially useful to understand the impact of crises, as it highlights how they create momentum in the problem stream, prompting the EU to address issues quickly. Its concept of “policy entrepreneurs” is also particularly relevant in Brussels, where stakeholders actively push their agendas in various institutions.

Figure 5: The Multiple Stream Model based on Kingdon—author’s graph¹⁶⁷



¹⁶⁴ Kingdon 2014.

¹⁶⁵ Cohen, March, and Olsen 1972.

¹⁶⁶ Ackrill and Kay 2011; Stocker, Stokmans, and Van Reisen 2022.

¹⁶⁷ Kingdon 2014.

The MSM highlights multi-causal interactions and the role of timing, emphasizing that successful policymaking involves aligning the streams in a non-linear and contingent process. It was thus particularly useful to make sense of parallel causal chains in the complex and dynamic context of the development of information governance in the EU. The MSM thus offers the opportunity to reconcile different assumptions about information challenges because it looks at the process before it looks at agents or intentions, a core weakness of misinformation policies and their theorizing. However, MSM offers loose categorisations that do not neatly organise data and causal factors, which can lead to confusion. Therefore, the project reduced the use of MSM as an analytical framework during the data collection and analysis processes, while keeping the structure of the subsequent thesis chapters chronological to enhance clarity.

5. Structure of the Dissertation

The remainder of this thesis is structured as follows. “Chapter 1—Undesirable Information in Cyberspace: Unpacking the Complexity of Propaganda, Misinformation, and Disinformation” makes important conceptual clarifications about undesirable information online, from a diplomatic studies perspective. It introduces the latest findings and debates in the field, highlighting the inter-disciplinary nature of information challenges and the necessary multi-faceted approach to address the issues they create, with lessons for both the study and practice of diplomacy related to information challenges. The next part answers the first two central questions of this thesis, i.e. *why EU counter-misinformation policies emerged the way they did, how they have evolved*.

“Chapter 2—Small State Influence in EU Security Governance: Unveiling Latvian Lobbying Against Disinformation” details how Latvia influenced EU information governance by leading a coalition to address pro-Kremlin disinformation following the 2013-14 Ukraine crisis. Its lobbying efforts led to the creation of the first joint EU measure against misinformation, the ESTF. To achieve this, Latvia leveraged its Council Presidency, NATO StratCom Centre of Excellence, and public momentum, securing funding from the European Parliament, and shaping long-term EU policies in the field of strategic communication.

“Chapter 3—Tackling COVID-19 Disinformation: Internal and External Challenges for the EU” examines the EU’s response to COVID-19-related information challenges. It highlights the shortcomings and difficulties of the EU’s approach, then mostly based on non-binding measures and a hands-off approach, in addressing interconnected internal and external challenges. Afterwards, the EU progressively strengthened its policy toolkit, not only with guidelines but also binding regulations and restrictive measures.

“Chapter 4—The Collective Securitisation of Disinformation and the EU’s Ban of *RT* and *Sputnik*” shows that the EU has progressively securitised misinformation, notably with the ban of *RT* and *Sputnik*, catalysed by Russia’s invasion of Ukraine. It highlights once again the central role of the Baltic states, as well as the growing role of the European Commission as an entrepreneur in information governance. This shift underscores a geopolitical turn in EU decision-making, raising concerns about transparency, democratic oversight, and restrictions

on the information space. Lastly, the chapter enhances collective securitisation, reflecting the insights from this case study on the theory as a whole.

Building on these four chapters, the final part answers the last research question, i.e. *which lessons we can draw from this case study about information governance*. “Chapter 5—Beyond Order and Disorder: A Grand Theory of Information Complex Systems” presents an innovative approach to understanding and responding to information challenges that questions the “order vs disorder” dichotomy that has guided misinformation studies and information governance, including in the EU. It advocates for a novel theory based on complexity science revolving around the key properties of complex systems: complementarity, feedback loops, uncertainty, and self-organization. It builds the ground for holistic, apolitical, global governance strategies that empower individuals, monitor trends, and address structural issues.

The Conclusion offers a summary of the dissertation, its core findings, contributions, limitations, as well as avenues for further research.