Humanities & Social Sciences Communications

ARTICLE

https://doi.org/10.1057/s41599-023-02179-8 OPEN

# The European approach to online disinformation: geopolitical and regulatory dissonance

Andreu Casero-Ripollés [1]✉, Jorge Tuñón [2] & Luis Bouza-García[3]

The COVID-19 health crisis and the invasion of Ukraine have placed disinformation in the focus of European policies. Our aim is to analyze the emerging European policy on counter-disinformation practices and regulations. To do this, we examine developing European Union (EU) strategy, against different forms of fake news, from a multidisciplinary approach that combines Journalism and Geopolitics. Our methodology is based on the critical analysis of documents generated by the EU on disinformation from 2018 to 2022, including reports, communications, statements and other legislative texts. Our findings suggest that the EU's policy against disinformation is based on two opposing logics that coexist and compete. The first is securitization, which understands this problem as a threat to democracy that legitimizes 'exceptional decision-making' from a hard power perspective. The second is based on the self-regulation and voluntarism of digital platforms with a clear orientation towards soft law and minimal intervention. The recent adoption of the Digital Services Act and the stronger regulation of online platforms do not replace this logic, since this legislation adopts a "co-regulatory framework". The coexistence of these two logics generates internal contradictions and dissonance that can determine the future of European policies on this important topic and its chances of success.

[1] Department of Communication Science, Universitat Jaume I de Castelló, 12071 Castelló, Spain. [2] Department of Communication Studies, Universidad Carlos III de Madrid, 28903 Getafe, Spain. [3] Department of Political Science and International Relations, Universidad Autónoma de Madrid, 28049 Madrid, Spain. ✉email: casero@uji.es

## Introduction

Following Russia's aggression against Ukraine on February 24, 2022, the European Union (EU) adopted a series of sanctions aimed at reducing Russia's ability to wage war. Whereas most were of an economic nature, measures suspending the airing in the EU of Russian government-controlled broadcasters, such as RT and Sputnik, were among the first EU reactions to the invasion. The rationale for these sanctions is that these broadcasters are sources of disinformation that are weaponized by the Kremlin: "Systematic information manipulation and disinformation by the Kremlin is applied as an operational tool in its assault on Ukraine. It is also a significant and direct threat to the Union's public order and security." (European Commission 2022) In doing so the EU took a further step, at least since the occupation of Crimea in 2014, towards its continuous consideration of Kremlin-sponsored disinformation as being part of a hybrid threat. Only one year earlier, in December 2020, the Commission took action on a different aspect of disinformation, the role of social media platforms in the spread and circulation of fake news, by including it among the content that platforms are required to remove when detected. This represented a real innovation, as previously the EU had expected platforms to comply on a voluntary basis.

The differences between these two regulatory elements show significant evolutions in the consideration of disinformation by the EU. Firstly, despite the incomplete transnationalization of public spheres (Rivas-de-Roca and García-Gordillo 2022), the EU sees disinformation as a multifaceted transnational phenomenon. Its policy response has in different moments addressed classical international concerns –the so called weaponization of disinformation in asymmetric conflicts (Szostek 2020)– globalization asymmetries –with transnational companies potentially exploiting regulatory asymmetries and differences between different policy blocs– and social transnational phenomena –distrust in media and authorities–, including scientists, and increased use of social media.

Secondly, disinformation is currently seen as a matter for regulatory intervention by the public sector, rather than an example of poor information supply that will be solved by the news market. As such, disinformation has experienced different 'international response regimes', going from the organization of international coalitions of professionals to counteract fake news, to its consideration as a security threat in the context of hybrid attacks. The consideration of such responses is fertile ground for analysis, since the analyses of responses adopted by international actors is as instructive as the areas in which action does not take place. The combination of these approaches allows for analysis of the emerging international regime of the fight against disinformation.

Finally, disinformation is a matter whose definition is the object of a broader struggle with implications for the media system, democratic institutions and international security. For instance, one of the legal and political implications of the suspension of RT and Sputnik broadcasting was 'what constitutes a broadcasting company that is protected by freedom of information and expression'. If the argument that government control of these outlets is the reason for their exclusion it may create precedents for public broadcasters in the EU. As such, it is the object of interest, competition and struggles between different interests.

The EU is both one of the actors and an arena upon which other actors intend to take action on disinformation. On the one hand, the EU institutions and member states have addressed fake news with different tools. On the other, actors such as social media platforms, third states and international journalism associations lobby the EU and its member states to act, or not act, upon specific aspects of the fight against disinformation.

These considerations demonstrate the need for a multidimensional and multidisciplinary approach to EU action on disinformation based on regulatory, sociological and journalistic approaches. In order to do so, this conceptual paper addresses the following question: what kind of struggles to define an EU regulatory response to the new 'disinformation order' are taking place in the field of European communication? The notion of disruption (Bennett and Pfetsch 2018) can be used to analyze how the crises of the 2010–2020 decade has contributed to making European public spheres more interconnected and impacting on EU integration. We argue that these crises, forms of contestation of EU issues and their management by EU institutions has contributed to enlarge the political arena beyond the national public spheres and include European issues on national agendas. This approach will be used to interpret the effects of the COVID-19 pandemic on the EU agenda and policy debate on disinformation: what strategy the EU should develop against different forms of disinformation in a post pandemic society? (Tuñón 2021) – and whether all these are equally important.

This paper builds upon previous work of the authors on the effects of the pandemic upon media consumption patterns (Casero-Ripollés 2020), and on the strategies of EU institutions to counter disinformation (Tuñón et al. 2019). To achieve this, it is based on a methodology of critical analysis of the documents generated by the EU on disinformation from 2018 to 2022, including reports, communications, statements and other legislative texts. Specifically, our paper analyzes three forms in which the EU has become concerned with disinformation: the intensification of news consumption, and disinformation circulation, during the COVID-19 pandemic; EU institutions attempts to develop soft law practices, supported by traditional and new media actors in tackling disinformation in the EU; and processes of securitization of disinformation carried out by EU institutions and member states. Whereas the fact that the EU policy on disinformation is the result of the convergence of different policy streams is by now a well-known fact (Ördén, 2020, Datzer and Lonardo 2022), less attention has been paid to the effects of the combination of these different policy tools. The central argument of the paper is the EU policy is characterised by a tension between what we call a geopolitical and a regulatory logic. The conception of the EU as a regulated, rationalised space where politics is subjected to norms and relations with an outside world seen as a jungle was famously openly presented by HR for foreign affairs and security Borrell in a speech in Bruges in 2022 (Borrell 2022). Postcolonial (Orbie et al. 2023) and critical geopolitical studies (Guzzini 2012) have highlighted that this conception is based on an ontological separation between how to deal with internal and external issues that potentially disrupts the ability of the EU to maintain its appeals to soft power (Wagnsson and Hellman 2018; Meunier and Nicolaidis 2019). Beyond the conceptual difference between these two logics that we discuss below we argue that they are rooted in an ontological self-understanding of the EU that can be traced back to its origins: a radical separation between the principles and norms that apply within and outside the EU political community. Our approach to these topics is theoretical and conceptual, not empirical. We adopt a multidisciplinary perspective to analyze this object of study that combines Digital Communication and Journalism with the vision of Geopolitics and Normativity.

## The current debate on disinformation and on policy responses: geopolitical and regulatory logics

Disinformation is nothing new in the history of journalism. On the contrary, its origins date back to the mid-20th century and are

connected to the development of propaganda (Freelon and Wells 2020). However, since 2016, with social media use, Brexit, and Donald Trump's victory in the US elections, it has grown massively (Waisbord 2018). Since then, the conditions for the creation, dissemination, consumption and impact of fake news have changed significantly. Now its volume is constantly growing, its circulation is increasingly rapid, its reach can be global, and the actors involved in its promotion are increasingly varied (Rúas-Araújo et al. 2020). Together, this represents a threat to the health of democracies.

The causes of the emergence of this new order of disinformation (Bennett and Livingston 2018) are diverse. One of them is the emergence and consolidation of social media, which have become a preferred platform for the circulation of false information due to their open nature and lack of controls and filters on the content in circulation. Another determining factor is the strong distrust of citizens towards mainstream media, whose credibility has been eroding for decades. This has led to a loss of authority in journalism (Carlson 2017), which has meant that the source of information is no longer a relevant criterion for the public. Consequently, traditional media have seen their influence as mediators reduced for a significant part of society. Newspapers or television have ceased to be a place where many people attribute relevance and reliability to news (Williams and Delli Carpini 2011). This has led to the collapse of the old news order and chaos in contemporary public communication (Waisbord 2018).

Another important ingredient is the configuration of a political landscape characterized by the dominance of post-truth. In this context, due to increased political polarization, citizens are more willing to accept arguments and information based more on their beliefs than on facts (McIntyre 2018). News consumption is thus becoming ideologically and emotionally driven and is responding to selective exposure rather than being the result of rational evaluation (Messing and Westwood 2014). Truth takes a back seat to the prominence of ideological consonance. To this scenario, it is worth adding the rise of political and media actors who resort to disinformation as a political strategy to achieve power. Thus, leaders and governments, on the one hand, and alternative media of a partisan nature (Holt 2020), on the other, become sources of false information that circulates freely through digital platforms. The cases of Donald Trump (Morini 2020) or Jair Bolsonaro (Ricard and Medeiros 2020) are examples of this type of practice.

The development of artificial intelligence and bots is also contributing to the consolidation of this new order of disinformation (García-Orosa 2021). These technologies significantly increase the ease, and reduce the cost, of producing fake news, even allowing the production of highly realistic misleading content by means of deep learning that resorts to AGN (antagonistic generative network) algorithms to manipulate existing images and videos, giving rise to deep fakes or ultra-fake information (Vizoso et al. 2021). Likewise, the emergence of key events, characterized by a highly disruptive component, drives the use and circulation of fake news. The window of opportunity that opens up in these cases to redefine previously established social constructions of reality makes these situations cardinal moments where the disinformative strategies of multiple actors are activated.

Disinformation has thus become a systemic challenge for democracies because of the combination of disruptive technological, political and sociological transformations of the public spheres in a very short period of time. Furthermore, the critical juncture effect is reinforced by a geopolitical zeitgeist that focuses on the vulnerability of democracies to structural transformations of the security order and the risks of global interdependencies. However, as we demonstrate in the following section, the COVID-19 pandemic and the Russian aggression on Ukraine demonstrate that notwithstanding the relation between the new security context and the global risk society the origins and nature of the disinformation threats remains different.

The rapid transformation of the public spheres and of the geopolitical environment are the context of the EU regulatory responses to disinformation. The fight against disinformation can seem quite distant from the issues typically associated with the EU. Probably only one decade before, this issue would have been left to member states because of its sensitive and divisive nature in relation to different values: for example, in the organization of media systems, and because balances between different liberties and forms of political contention are very different across Europe (Hallin and Mancini 2004, Humprecht 2019), and thus typically a national issue.

One of the legacies of the atypical nature of disinformation as a policy issue for the EU is the dilemmas it creates for the international role of the EU. Existing literature has pointed out different tensions and trade offs that the fight against disinformation introduces in the EU's self-perception as a civilian power (Wagnsson and Hellman 2018) which enhances narratives of ontological insecurity (Della Sala 2018), risks justifying censorship or a transformation of public spheres towards more dialogic positions such as pro or anti-EU (Ördén 2020) and promotes a language of information war that undermines the EU ability to carry out public diplomacy (Szostek 2020).

As argued below, the EU policy on disinformation responds essentially to increasing aggressiveness of Russia and to the effects of the COVID-19 pandemic. Whereas policy innovation in response to converging streams is the classic Kingdon model of policy change (Kingdon 1984), existing literature does not sufficiently focus on the policy tensions that the combination creates. In Kingdon's model, policy change happens when policy, political and problem streams converge. However, this takes time and reformulation. Even though authors like Datzer and Lonardo (2022) argue that the geopolitical origin does no longer operate, we argue there is a tension between regulatory and geopolitical logics. The geopolitical logic is one that conceives disinformation as a weapon used by foreign rivals or enemies to exploit the vulnerability of democratic publics to manipulation and interference. This approach conceives pluralism and openness as a potential vulnerability (Szostek 2020) and as result considers it acceptable to witness a stronger public intervention of the public sphere. This intervention can range from active monitoring, exposure and criticism of foreign campaigns to a more regular information control by security services (European Commission and High Representative on Foreign Affairs and Security Policy (2018) and to information censorship (Council of the European Union 2022). On the other hand, the regulatory logic conceives disinformation as an undesired result of an otherwise positive - in economic, cultural and economic terms - tendency to digitalisation of the public spheres. In this sense the main rationale for the origin of disinformation is the competition for the attention of publics in a distorted digital attention market and the issue can be tackled by public and private efforts at demonetisation, digital alphabetisation and fact-checking (European Commission 2018b).

Obviously, both threats can live side by side and some of the policies are not by design incompatible (intelligence services can collaborate with fact-checkers). However we argue that the combination of these two policy logics shows similar tensions to the ones the EU has experienced in the regulation of the digital ecosystems: because of the "EU's considerable economic and regulatory power in digital matters and its limited mandate and capabilities in foreign policy" (Broeders et al., 2023: 1), there is a potential for a mismatch between the hybrid usage of market

regulation policies - such as competition or self-regulation - while an exceptionality logic prevails elsewhere.

In this line, the paper contribution consists in pointing out two such gaps that are only being addressed now. Firstly, the securitization of disinformation, accelerated by the war in Ukraine, decreases the policy space for policy communities and solutions focused on pluralism that, as argued above, were already weak in the EU policy community such as media professionals (Ördén, 2020). Secondly, security speech acts focused on the designation of information as a weapon and on pluralistic debate as a vulnerability (Szostek 2020) not only risk undermining democratic public spheres (Ördén, 2020) but also make other definitions of the problem invisible.

## Crisis and disruption of global and transnational public spheres

**COVID-19**. COVID-19 has maximized the circulation of disinformation (López-García et al. 2021). The need to obtain data and knowledge about the progress of the virus and how to combat it generated a big increase in interest and news consumption (Casero-Ripollés 2020). In this context, disinformation increased significantly. Between January and October 2022, the International Fact-Checking Network (IFCN) detected 21,018 misleading reports about the Coronavirus worldwide. This volume led the World Health Organization (WHO) to classify this phenomenon as an 'infodemic' (Gabarron et al. 2021). False news about this health crisis fell into four main areas: the causes of the appearance of the virus; the disease itself (symptoms, transmission and consequences); the treatments and ways of curing it and, finally; the intervention and action of public authorities in the face of this crisis (Salaverría et al. 2020).

COVID-19 has stimulated disinformation (Salaverría et al. 2020; López-García et al. 2021). The potential political effects on democracy of fake news about the pandemic along with its consequences on health and human lives have provoked a two-pronged response from journalists (Casero-Ripollés 2021, De Sousa et al. 2022). On the one hand, verification has been boosted with the emergence and consolidation of media and platforms dedicated to checking the veracity of information. Some of the leading examples are Chequeado, Snopes, Full Fact, Pagella politica, Newtral or Maldita, among others (García-Vivero and López-García 2021). The magnitude of the phenomenon has led to the creation of the International Fact-Checking Network (IFCN), under the auspices of the Poynter Institute in 2015. These media focus their activity on debunking fake news and hoaxes through fact-checking. These organizations do not produce news but verify it. The most common types of information they work with are election promises, interviews and debates, statements by politicians, data used by parties or governments and content disseminated on social media, particularly on mobile instant messaging services such as WhatsApp (Vázquez-Herrero et al. 2019). The increased importance given to verification has also led generalist media to incorporate sections or spaces within the media dedicated to checking data to detect falsehoods and inaccuracies. Some examples, in Europe, are Les Décodeurs, from Le Monde (France), BBC Reality Check, from the British Broadcasting Corporation (United Kingdom) or EFE Verifica, from Agenda EFE (Spain), among others (García-Vivero and López-García 2021).

Secondly, the Coronavirus pandemic has accentuated collaboration between media, verifiers and digital platforms. Previous initiatives included Cross Check, which in 2017 united 37 French media to check news during the election campaign, or First Draft, which was created in 2015 by Google, Facebook, Twitter, the Open Society Foundation, among others, to protect citizens from disinformation and empower them to identify and avoid hoaxes. However, COVID-19 has accelerated such dynamics. The large volume of fake news in circulation, the complexity of the situation, the economic cost of verification and the need to provide rapid responses have encouraged new forms of cooperation. One of these is the #CoronaVirusFacts Alliance which, since January 2020 under the leadership of the IFCN, brings together more than 100 verifiers from around the world to tackle misinformation about the pandemic. Another is Latam-Chequea-Coronavirus, a collaborative project that brings together 40 Latin, Spanish and Portuguese media. This latter case, in addition to comparing information with a common methodology, presents the novelty of offering access to the data obtained in open format. They have also created a board game, called 'Truth or Hoax? Coronavirus Edition', to curb disinformation through gamification, which can be downloaded free of charge on the Internet. For their part, the main social media and technology companies, such as Facebook, Google, Twitter, Microsoft and Reddit, announced their union to fight against fake news after the start of this health crisis. In addition, some of these digital media, such as WhatsApp, have provided donations to fund the activity of the verifiers. These actions highlight the importance and necessity of cooperation between journalists, media and platforms to combat misinformation and strengthen the reach and power of fact-checking, especially at critical times such as COVID-19.

**War in Ukraine**. If COVID-19 exponentially multiplied the spread of disinformation, something similar has happened as a consequence of the latest major crisis, the War in Ukraine, following the Russian invasion in February 2022. Indeed, one of the main components of hybrid warfare is information warfare, which seeks to gain informational advantages over the enemy (Carrión 2022), now in a much more sophisticated form (Lucas and Pomeranzev 2016). This allows not only information control and censorship, but also the dissemination of disinformation in the form of false, decontextualized or misleading information through digital platforms (Morejón-Llamas et al. 2022). These activities are carried out with the aim of reinforcing one's own image or counteracting that of the adversary and are closely linked to another of the strategies that make up hybrid warfare: psychological warfare.

As reflected by the Council of the European Union (2022), systematic information manipulation and disinformation have been applied by the Russian government as an operational tool in its assault on Ukraine. Something that researchers such as Milosevich-Juaristi (2017) had already analysed thematically before the conflict began in 2022. She pointed to the segmentation of Russian disinformation narratives according to their audiences: internal or domestic; neighbouring ones referring to the post-Soviet space; and Western ones. This has been endorsed (after the invasion) by other researchers, which admit that (nowadays) the contenders have the potential to disseminate instant disinformation (Wagner and Degli-Esposti 2022), and have been doing so, not only to attack, but also, in a novel fashion, to defend themselves, thus seeking to gain the favor of public opinion since the beginning of the conflict (Montes 2022).

In fact, it is a continuation of the post-Soviet propaganda strategy (Magallón-Rosa 2022, Morejón-Llamas et al. 2022), characterized by: information intoxication, enemy exhaustion, inoculation of distrust in leaders, intensification of dissension between social classes, incrimination of the enemy and propagation of threats (Stancu 2019). A campaign that has been intensified after the annexation of Crimea in 2014, with the invasion of Ukraine in 2022 as its climax (EuvsDisinfo 2022), through the segmentation of its audiences. In fact, research such

as that of Nimmo et al. (2020) confirm that between 2014 and 2020, the Russian disinformation campaign produced at least 2.500 pieces of disinformation content in seven languages and more than 300 platforms through fake accounts and forged documents to sow conflict among Western countries and justify an eventual attack on Ukraine.

Regarding the subject matter, a large part of the hoaxes distributed by Russia are framed within the rhetoric of the alleged existence of a 'Russophobic and Nazi' government in Ukraine that is committing genocide against Russian citizens. A narrative clearly reminiscent of the Second World War (Fortuin 2022). In relation to the format, a consolidation of disinformation techniques can be observed, through the production of attractive content, including fabricated stories that use and adapt photos and videos according to the narrative requirements. Thus, entertaining, emotionally appealing lies are produced that fit perfectly with a preconceived narrative and the confirmation biases of the target audience (Lucas and Pomeranzev 2016).

In the face of this Russian disinformation offensive in Ukraine, the European Union has counted more than 1.200 separate cases in 2022 alone (Europa Press International 2022). It has also imposed sanctions and measures against Russian propagandists and disinformers, suspending from 2022 the broadcasting licenses and activities on European territory of several companies or disinformation media arms of the Kremlin's. This measure has caused some controversy in Europe, as it contravenes the traditional and long-standing European policy of freedom of the press.

Beyond the above initiatives, the EU continues to invest efforts in: media literacy of citizens about Russian disinformation, through the EUvsDisinfo project, founded for this purpose in 2015; public awareness of disinformation and coordination of better responses among member states through the Rapid Alert System (linked to the EU's External Action Service) since 2020; or the analysis and monitoring of disinformation narratives across the conflict through the European Digital Media Observatory (EDMO), a network attached to the European Commission and consisting of verifiers, media literacy experts and academic researchers (OECD, 2022).

Summing up, Russia's unprovoked aggression against Ukraine is well known for the extent to which it is being fought and shared online. While social media had played a role in previous wars (the annexation of Crimea in 2014 included), Russia's full-scale invasion of Ukraine (2022) has illustrated how social media have changed the way war can be narrated, experienced and understood (The Economist 2022). This is a clear consequence of the exponential world-wide increase in internet coverage and the use of social media. Therefore, while "the use of disinformation as a weapon has always existed, the social media landscape has multiplied its potential reach and penetration" (OECD, 2022: 1).

Indeed, the massive disinformation flows surrounding the invasion of Ukraine in February 2022 have marked an obvious turning point in the escalation of Russian disinformation operations towards not only Ukraine but also Western democracies. In particular, disinformation narratives have evolved from propaganda and historical revisionism (i.e. Crimea was always Russian) (Coynash 2021; Chotiner 2022) to Manichean claims of a neo-Nazi Ukrainian government or conspiracy theories of American-Ukrainian biological weapons laboratories during 2022.

"The flow of – and disruption caused by – Russian disinformation has significantly increased since Russia's invasion in February 2022. In turn, Ukraine's response to the Russian disinformation threat has built upon progress made in strengthening the information and media environment since 2014 and in establishing mechanisms to respond directly to information threats. These include efforts to provide accurate information, ensure that media organisations can continue operations, and policy efforts to combat the threats posed by Russian state-linked media" (OECD, 2022: 2).

In response, the EU has recently strengthened its geopolitical logic towards disinformation (as introduced in Section 2 and fully discussed in the following ones, 4 and 5) by means of unprecedented and controversial approaches. We are referring to the restriction of access to Russian propaganda tools (weapons used by foreign rivals or enemies to exploit the vulnerability of democratic publics to manipulation and interference, as stated by Szostek 2020) such as Sputnik or Russia Today. But also, the legislative developments in the European Media Freedom Act - with unprecedented action in a field close to Member states identity - and the Digital Services Act definitions of legal but harmful content. Explaining this requires pointing out how Russian aggressiveness is at the origin of the geopolitical turn, whereas the COVID – 19 internal disruptions explain the logic of the EU towards regulation.

## The fragmented approach of EU institutions to disinformation

For some time now, the European Commission seems to have been aware of the need to defend the European project from hybrid strategies and disinformation attacks. Since 2015 the European Council defined Russian disinformation and responded with the creation and further strengthening of the EastStratCom Task Force (Wagnsson and Hellman 2018) with the objective to detect and respond to disinformation using strategic communication (Ördén, 2020). It is not until 2018, however, that the Commission developed a more comprehensive series of ad hoc initiatives and policy documents, meaning that the original policy community that introduced disinformation in the EU agenda is the security one (Ördén, 2020). By 2018 the European Commission had launched a Eurobarometer public opinion survey and a public consultation, in addition to setting up a High-Level Group and, later, publishing a Communication and a Code of Conduct.

Ördén (2020: 422) found four possible policy solutions that have been discussed in different EU fora: strategic communication, censorship, media literacy and media pluralism. However, the result of this origin in the security community is that the EU has addressed online risks as part of a hybrid threat challenging security values and emphasised security centered solutions. This does not mean that censorship - or for that matter strategic communication (Szostek 2020) - are the dominant policies, but that content control in the form of decreased visibility is today a more likely solution than in previous decades (Rone, 2021: 176).

The measures that the EU has adopted highlight the vulnerability of democracies and the European project to manipulation of their electoral processes by foreign powers, especially Russia (Szostek 2020). The key actor in the development of this perspective has been the European External Action Service (EEAS), which since 2015 has been home to the East StratCom Team, a communications team that collaborates with fact checkers and foundations to denounce the dissemination of fake news by Russia in the eastern states, in the context of the EU's neighborhood policy. This work was formalized on May 12, 2018, with the adoption of the Disinformation Action Plan, which linked fake news to destabilization processes typical of hybrid attacks (European Commission-High Representative CFSP 2018d: 11-12). This document encompassed disinformation in the context of hybrid threats faced by the EU and its member states, formalized communication teams such as the aforementioned East StratCom and strengthened EU services seeking cooperation with the EEAS on social media and fact checkers who are signatories to

the above-mentioned code. However, the document paid scant attention to the role of journalists and the media (Tuñón et al. 2019).

Instead, issues related to media pluralism and education in Ördén's terms, were first addressed by the High-Level Group on fake news and disinformation online (composed of representatives of social media and technology companies, verifiers, media, academics and members of civil society). This group was tasked with drafting a report of the High-Level Group on fake news and disinformation online' (European Commission, 2018a, b). From a European institutional perspective, the Report aimed at defining and quantifying disinformation, as well as studying possible legal mechanisms and countermeasures to combat it. The document suggested focusing on: the transparency of news and its circulation online (creation of credibility algorithms); media and digital literacy; the empowerment of users and journalists to combat disinformation (collaboration with independent verifiers); the sustainability of the media ecosystem (elimination of advertisements on websites that propagate disinformation); and the evaluation and monitoring of the solutions offered to verify their effectiveness (Tuñón et al. 2019:148). Despite being non-binding, the Report was largely reflected in the subsequent European Commission Communication of April 26, 2018, on "Combating online disinformation" (European Commission 2018b), which was the starting point for all European policy initiatives that flourished during 2018 and 2019, mainly in the run-up to the last European Parliament elections.

The Commission's intention was to give digital media, social network sites or internet advertisers a reasonable period of time to adapt to the Report and the Communication, before considering further legislation on disinformation. Although it was only a non-binding document, the Commission promoted the 'European Code of Practice on Disinformation' (European Commission 2018a) as a self-regulatory agreement. In this agreement, actors such as Facebook, Google, Mozilla and Twitter committed on September 26, 2018, "to self-regulatory standards, to make political advertising more transparent or to introduce data verification mechanisms, in order to fight disinformation in the framework of the European elections in May 2019 and other future electoral processes". Specifically, companies pledged to encourage more transparency in political advertising; shut down fake accounts or discredit disinformation providers; invest in technologies and programs such as "trust indicators" to help citizens make informed decisions; use technology that prioritizes "relevant, authentic and authoritative information"; and work with civil society and governments to "improve critical thinking and digital media literacy".

There is no doubt that in the run-up to the 2019 European Parliament elections and against the background of the Brexit referendum and the 2016 American presidential elections (but also as a result of the monitoring of various state and sub-state elections in the member states), the EU devoted considerable time in 2018 to developing various initiatives to help prevent disinformation from sweeping Europe. Once the critical moment of the 2019 European elections had passed, within the framework of initiatives derived from the Action Plan against Disinformation (such as the stimulation of the role of platforms or the establishment of verification and/or early warning systems for disinformation, such as https://eufactcheck.eu/), in the summer of 2020 all the milestones achieved to date were evaluated and the capacities of https://eufactcheck.eu/ were reviewed from the perspective of respect for fundamental rights, literacy, communication, cooperation and the promotion of transparency. The aim was to optimize this fake news verification unit, in conjunction with the right to the free communication of truthful information. This was intended as a prelude to the latest major European legislative milestone in the fight against disinformation, the recent Action Plan for European Democracy (December 2020), which was conceived as a European response to the vulnerabilities detected in the infodemic context of COVID-19 since 2020.

With the most recent basic theme of disinformation strategies being the pandemic itself, the Action Plan for European Democracy (European Commission, 2020) rests on three pillars: the promotion of free and fair, as well as transparent, elections; the strengthening of media freedom and pluralism; and the fight against disinformation (in the form of co-regulation, through the law on Digital Services, which the EU adopted in April 2022). This suggests that the pandemic opened a window of opportunity to pay attention to the issues of pluralism (Ördén, 2020) that had been neglected in the original security agenda. On the one hand, for the first time the EU regulates online platforms (beyond voluntary cooperation) because of the Digital Services Act, and cooperation includes disinformation as one of the systemic risks that platforms must act against. On the other, the Action Plan for Democracy is therefore a milestone in the European approach to disinformation, insofar as it moves from considering it a mere threat to security to giving it the status of one of the three pillars of defense of European democracy. The political significance of the Plan, which should be the Community tool that will provide the backbone for policies in this area until 2023, is clear. Beyond the other two pillars (promoting free and fair elections and strengthening media freedom and pluralism), the fight against disinformation involves improving European instruments to counter foreign interference, including the possibility of imposing sanctions on those responsible, in accordance with European values and principles. The objectives are to improve European capacities (both EU and member states) to combat disinformation, to create responsibilities and obligations for online platforms, and to empower European civil society through the promotion of media literacy. In short, the third pillar of the Action Plan aims (even through the imposition of sanctions on those responsible) to increase transparency, crack down on manipulation techniques and reduce the economic incentives derived from the dissemination of disinformation.

## The EU's geopolitical turn and the tension between securitization and collaborative approaches to disinformation

The EU's geopolitical turn is a central issue in ongoing debates of European politics both in academia (Cadier 2019; Meunier and Nicolaidis 2019; Oleart, Bouza-García 2019) and in politics, as evidenced in national leaders' debates and speeches in the European Parliament in recent years (Macron 2018; Merkel 2018). In his opening speech in the European Parliament Mr Borrell, the High Representative for Foreign Affairs and Security Policy, declared that "the EU must learn to use the language of power" (Borrell 2019).

Furthermore, the approach of this agenda to the EEAS would also surprise some, as political entrepreneurs in this area –journalists, civil rights activists, political campaigners–, would be more likely to seek the involvement of Commission Directorate-Generals with internal regulatory competences, such as DG Competition or DG Justice. As an example, increased concerns about the effect of disinformation on democratic processes has favored the organization of generally liberal and left-of-centre national and transnational communities of fact-checkers (Shin and Thorson 2017; Lyons et al. 2020) that denounce disinformation as part of national-populist strategies (Rivas-de-Roca et al. 2023), both in the US and the EU.

We argue that a process of securitization in the fight against disinformation is happening in the EU. This consists of a series of

security-related 'speech acts' that firstly requires that a fundamental good is threatened (Wæver 1995), in this case democracy, and that exceptional measures are required to protect it. This is the process that makes disinformation not an issue for media professionals – if emphasis was put on the public sphere – or competition lawyers – if emphasis was put on the dissemination of disinformation in a few platforms – to address, but one to be put in the hands of traditional security officials. In this scenario, fake news becomes part of the broader security landscape of contemporary societies (Monsees 2020). Despite the clear signaling of the risks of addressing disinformation as a threat, the literature has not explicitly used the securitization theory (but see Daniel and Eberle 2021 for a case study of the Czech Republic). Focusing on speech acts is particularly important since, as argued by Szostek (2020: 2732-2734), assuming that information can be weaponised to target vulnerable audiences with strategic results is far from obvious and thus requires an elaboration that can work in a context of exceptionality. In this sense, the EU decision on Sputnik and Russia Today is an example of a logic of exceptionality making a direct connection between the spread of propaganda and security:

> "(8) Those propaganda actions have been channeled through a number of media outlets under the permanent direct or indirect control of the leadership of the Russian Federation. Such actions constitute a significant and direct threat to the Union's public order and security." Council of the European Union 2022.

This is an example of a speech act under a logic of exceptionality since in other circumstances the link between spread of propaganda and security would require several intermediary steps (a less informed public, biased elections, uninformed policy decisions etc.) that are not elaborated upon.

The logic of exceptionality is a cornerstone of securitization theory: when an issue is designated as a threat, it is no longer dealt with through the ordinary policy channels. However, this requires two qualifications when applied to the EU. Firstly, the exceptionality logic may in itself be a requirement for the adoption of new policies by the EU according to the well-known idea that EU integration advances through crises. Secondly, exceptionality in the EU usually means that member state policy professionals are associated more closely with decision-making than in "normal" EU policies. The aforementioned EEAS strategy against disinformation effectively reserves an important role for member states to specialize in regional disinformation and interference strategies.

Finally, the geopolitical turn also has an identity-building dimension: European threats are shared, and as a result responses represent more than a new policy but a shared struggle against a common enemy. As highlighted by Guzzini (2012: 6), geopolitical discourse has a tendency to essentialize identities. This contributes to the securitization strategy: all disinformation originating in Russia, China or Iran is identified with a state attack against the EU, whereas some of these may come from para or non-state actors and not necessarily be targeted at the EU as such, but at member states, companies or political actors. Instead, the geopolitical approach makes the threat broader and pits states, and beyond those alliances, against each other.

The European response to the disinformation dimension of the Ukraine invasion is an excellent illustration of this process of securitization. The reference by Borrell (European Commission 2022) makes a direct (literally in the quote) link between disinformation and threats to public order and security. It follows a logic of exceptionality in that EU institutions themselves are aware that an executive ad hoc suspension of a legally attributed broadcaster sets a dangerous precedent, which they negate in legally uncertain ground:

> "(11) Consistent with the fundamental rights and freedoms recognized in the Charter of Fundamental Rights, in particular with the right to freedom of expression and information, the freedom to conduct a business and the right to property as recognized in Articles 11, 16 and 17 thereof, these measures do not prevent those media outlets and their staff from carrying out other activities in the Union than broadcasting, such as research and interviews." (Council of the European Union 2022).

Finally, the decision on RT and Sputnik evidences the geopolitical reading of the intentional, strategic, state-led and aggressive content of all content from these channels, as well as defining Russian propaganda as the antithesis of EU values:

> "The Russian Federation has engaged in a systematic, international campaign of media manipulation and distortion of facts in order to enhance its strategy of destabilization of its neighbouring countries and of the Union and its Member States. In particular, the propaganda has repeatedly and consistently targeted European political parties, especially during election periods, as well as targeting civil society, asylum seekers, Russian ethnic minorities, gender minorities, and the functioning of democratic institutions in the Union and its Member States" (Council of the European Union 2022).

The EU response to disinformation has been paradoxical. On the one hand, it has adopted a hard power approach in the EEAS strategy that includes the use of acronyms highly reminiscent of geopolitical thought, such as the East StratCom, and is well exemplified in the following quote:

> "disinformation campaigns by third countries can be part of hybrid threats to internal security, including election processes, in particular in combination with cyberattacks. For example, Russian military doctrine explicitly recognizes information warfare as one of its domains" (European Commission 2018a, b: 2).

However, on the other hand the EU has not adopted any type of mandatory policy towards online platforms and social media companies such as Facebook or Twitter until the agreement on the Digital Services Act (DSA) discussed above. Before this policy turn related to the COVID-19 crisis, the EU followed a consensual approach via a High-Level Group on Fake News and Online Disinformation:

> "All relevant stakeholders, including online platforms, news media organizations (press and broadcasters), journalists, fact-checkers, independent content creators and the advertising industry, are called upon to commit to a Code of Practices." (High-Level Group on Fake News and Online Disinformation 2018).

The recommendation of this group resulted, a few months later, in a self-regulatory Code of Practice, which has now been strengthened following the adoption of the DSA. However, the regulatory dimension of the DSA has not totally changed the self-regulation approach: "The DSA will set out a co-regulatory framework, including through voluntary Codes of Conduct or other co-regulatory measures, aimed at addressing systemic risks by the Very Large Online Platforms, including those linked to Disinformation." (European Commission 2022). This contrasts with the case of Germany, which in 2017 adopted the NetzDG law that demands that platforms of a certain size delete illegal content,

related to disinformation and hate speech, within 24 hours and non-compliance leads to high penalty fees (Monsees 2020).

Beyond the issue of whether or not private for-profit companies and private interests should be cornerstones in the fight against disinformation in the EU, it must be underlined that, while the Commission is increasingly trying to make demands on digital platforms to combat the viralization of false or/and biased content, industry executives claim that it is not their responsibility to control online material, which is not predominantly technically illegal. Likewise, social media companies have also partnered with EU fact-checkers to debunk false reports on their networks, although to date such partnerships have had minimal impact in precisely targeting false narratives.

At first glance this challenges the aforementioned interpretations on the geopolitization and securitization of disinformation issues in the EU. It can hardly be argued that there is a move towards a regime of exceptionality considering that elements of this logic coexist with forms of stakeholderism and soft law typical of neoliberal governmentality (Heiskala and Aro 2018). This is backed by the fact that these two radically different approaches emerge from two different services, the EEAS for the former, DG Connect for the latter, reflecting different institutional practices. When applied to the new issues of disinformation this division creates a situation where fake news coming from non-Western sources is associated with state strategies and foreign political interference and must be addressed as a security threat, whereas disinformation associated with US technological players such as Facebook is understood to be the product of a broader transformation of the media and news market and must thus be dealt with via traditional liberal and market tools.

## Conclusion

Our findings allow us to make original and relevant contributions regarding the role of the European Union (EU) in the fight against disinformation. The increase in the intentional and harmful use of this type of content during COVID-19 and the invasion of Ukraine has increased the strategic relevance of this problem. Our analysis reveals that European policies on this issue are in the process of redefinition in the post-pandemic scenario and are facing significant internal contradictions.

Our first contribution is to confirm that disinformation has increased in importance on European policy makers' agenda. Since 2018, the EU, first due to concerns about its impact on the elections to the European Parliament in 2019 and, later, due to its role in the COVID-19 health crisis, has promoted a number of initiatives to tackle this problem. These actions have predominantly been based on self-regulation and the shared responsibility approach. The EU is striving to achieve greater commitment and involvement of private digital platform companies in relation to the fight against fake news. These platforms, however, have been reluctant to assume greater responsibility, in in line with their capitalist and neoliberal nature. In this context, a soft law-oriented policy with few demands and obligations for digital platforms prevailed until the pandemic, beyond codes of good practice and voluntary formulas. Proof of the scarce interest of these companies in assuming a front-line position is their strategy of outsourcing the fight against disinformation. By providing financing and seeking alliances with fact-checkers, they push the problem and responsibility towards a third party. The great challenge of European policy will be how to achieve strong commitment from digital platform companies in the struggle against fake news, as they are key players in this problem, even though they perceive it as being far from their responsibility. The Digital Services Act addresses this issue in a mandatory way by forcing platforms to increase the transparency of their content moderation and include information in their new risk self-assessment by establishing sanctions for lack of action. On the other hand, the action to be taken will remain the object of co-regulation via the pre-existing rationale of codes of practices mentioned above.

At the same time, the EU has sought to encourage the promotion of fact-checking and media literacy (Tuñón et al. 2019). These are relevant actions, but both have a medium- or long-term results' horizon. Furthermore, commitment to the former also has an effect on an ongoing policy discussion, since fact-checking is more problematic than the EU seems to assume: denouncing fake news may not only fail to persuade, but often reinforce it because of what psychologists call "confirmation bias"; the instinct to accept what aligns with preconceived beliefs, for example, by repeating the anti-EU Euro myth, as happened in the UK. An alternative strategy to combat disinformation on the part of both political actors and the media would be the promotion of alternative frameworks. This option has its advantages in the long run, given that 'whoever frames first' usually wins the discursive dispute in the public sphere.

On the other hand, our second contribution is to identify that a geopolitical turn is taking place in EU policy against disinformation. A process of securitization consisting of applying security tools and discourses - upon an object that was previously not identified as such - is being promoted. This means that security community actors – the military, police, state information services, security consultants – are being brought into policy areas, such as the fight against fake news, which was previously dominated by actors in the public sphere, such as media companies or journalists. Under this perspective, in the EU context, disinformation is conceived as a threat to European democracy. Fake news, especially that from Russia, China or Iran, are conceived as a threat to democratic health and as a strategic resource in information warfare. This makes it a global problem and not just limited to a professional group, such as journalists, or to a single member country. It therefore takes on an international dimension and becomes a key geopolitical element for the EU. Consequently, it requires extraordinary measures involving the activation of a logic of exceptionality. The EU's response to the Ukraine invasion is an example of this. In this context, disinformation is an exceptional security issue, placing it at the centre of European policy priorities.

Consequently, two opposing logics, securitization and self-regulation, coexist and compete when determining the focus and political actions of the EU against disinformation. This contrast between a vision of hard power, facing a cardinal threat, and another of soft law, based on voluntarism and minimal intervention in the digital media industry, generates dissonance. As a result, the EU is being accused at the same time of promoting a strong discourse linking disinformation to security, exceptionality and geopolitical strategies, and being lax with the obligations and responsibilities of the digital platform companies. This has led to a significant internal contradiction that the new DSA may only now be starting to address. Its resolution will be key to determining not only future EU policies on this topic, but also conditioning its chances of success in the face of an increasingly growing problem for European democracy.

Received: 30 October 2022; Accepted: 20 September 2023;
Published online: 06 October 2023

## References

Bennett WL, Pfetsch B (2018) Rethinking political communication in a time of disrupted public spheres. J Commun 68(2):243–253. https://doi.org/10.1093/joc/jqx017

Bennett WL, Livingston S (2018) The disinformation order: disruptive communication and the decline of democratic institutions. Eur J Commun 33(2):122–139. https://doi.org/10.1177/0267323118760317

Borrell FJ (2019) Hearing of Josep BORRELL FONTELLES, High Representative/Vice President - Designate of the European Commission: Opening Statement by Josep BORRELL FONTELLES. Committee on Foreign Affairs (AFET), European Parliament: Brussels, October 7, 2019. https://multimedia.europarl.europa.eu/en/video/hearing-of-josep-borrell-fontelles-high-representative-vice-president-designate-of-the-european-commission-opening-statement_I178140 Accessed 15/07/2022

Borrell FJ (2022) EU Ambassadors Annual Conference 2022: Opening speech by High Representative Josep Borrell. The European Union official website. https://www.eeas.europa.eu/eeas/eu-ambassadors-annualconference-2022-opening-speech-high-representative-josep-borrell_en Accessed 14/09/2023

Broeders D, Cristiano F, Kaminska M (2023) In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. JCMS: J Common Mark Stud 61(5):1261–1280

Cadier D (2019) The geopoliticisation of the EU's Eastern Partnership. Geopolitics 24(1):71–99. https://doi.org/10.1080/14650045.2018.1477754

Carlson M (2017) Journalistic authority: Legitimating news in the digital era. Columbia University Press, New York

Carrión J (2022) Estamos ante la Primera Guerra Mundial Digital. Inspirar y Transgredir, 17. https://comunicacion.gumilla.org/wpcontent/uploads/2022/09/com_98_17-20.pdf

Casero-Ripollés A (2020) Impact of COVID-19 on the media system. Communicative and democratic consequences of news consumption during the outbreak. Profesional de la información 29(2). https://doi.org/10.3145/epi.2020.mar.23

Casero-Ripollés A (2021) The impact of COVID-19 on journalism: A set of transformations in five domains. Comunicação e Sociedade 40:53–69. https://doi.org/10.17231/comsoc.40(2021).3283

Chotiner I (2022) Vladimir Putin's Revisionist History of Russia and Ukraine, The New Yorker, https://www.newyorker.com/news/q-and-a/vladimir-putins-revisionist-history-of-russia-and-ukraine

Council of the European Union (2022) Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine OJ L 65, 2.3.2022, p. 1–4. http://data.europa.eu/eli/reg/2022/350/oj Accessed 15/07/2022

Coynash H (2021) Moscow's Proxy "Republics Announce That Donbas Is and Always Was Russian, Kharkiv Human Rights Protection Group, https://khpg.org//en/1608808705

Daniel J, Eberle J (2021) Speaking of hybrid warfare: multiple narratives and differing expertise in the 'hybrid warfare' debate in Czechia. Cooperation Conflict 56(4):432–453. https://doi.org/10.1177/00108367211000799

Datzer V, Lonardo L (2022) Genesis and evolution of EU anti disinformation policy: entrepreneurship and political opportunism in the regulation of digital technology. J Eur Integr: 1–16. https://doi.org/10.1080/07036337.2022.2150842

De Sousa V, Capoano E, Rodrigues Costa P, Paganotti I (2022) ¿La Covid-19 ha infectado las noticias? Cómo los periodistas, las audiencias y los procesos de producción son alterados por las pandemias. Universitas-XXI, Revista de Ciencias Sociales y Humanas 37:19–41. https://doi.org/10.17163/uni.n37.2022.01

Della Sala V (2018) Narrating Europe: the EU's ontological security dilemma. Eur Security 27(3):266–279. https://doi.org/10.1080/09662839.2018.1497978

Europa Press Internacional (2022, 24 octubre). La UE lanza una nueva herramienta para combatir el auge de la desinformación rusa por la agresión a Ucrania. https://www.europapress.es/internacional/noticia-ue-lanza-nueva-herramienta-combatirauge-desinformacion-rusa-agresion-ucrania-20221024131117.html Accessed 14/07/2022

European Commission (2018a) Code of Practice on Disinformation. Europa Website. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation Accessed 15/07/2022

European Commission (2018b) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling Online Disinformation: a European Approach COM/2018/236 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236 Accessed 15/07/2022

European Commission (2022) Press release Ukraine: Sanctions on Kremlin-backed outlets Russia Today and Sputnik Brussels, 2 March 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1490 Accessed 15/07/2022

European Commission and High Representative on Foreign Affairs and Security Policy (2018) Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation (JOIN(2018) 36 final). Brussels, 5. 12. 2018. https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation Accessed 15/07/2022

European Commission (2020) Communication on the European democracy action plan COM/2020/790 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423 Accessed 16/07/2022

EuvsDisinfo (2022) Key Narratives in pro-Kremlin Disinformation part 1: the Elites v the People. https://euvsdisinfo.eu/key-narratives-in-pro-kremlin-disinformation-part-1-the-elites-v-the-people/ Accessed 28/07/22

Fortuin E (2022) Ukraine commits genocide on Russians: the term "genocide" in Russian propaganda. Russ Linguist 46(3):313–347. https://doi.org/10.1007/s11185-022-09258-5

Freelon D, Wells C (2020) Disinformation as political communication. Political Commun 37(2):145–156. https://doi.org/10.1080/10584609.2020.1723755

Gabarron E, Oyeyemi SO, Wynn R (2021) COVID-19-related misinformation on social media: a systematic review. Bullet World Health Org 99(6):455. https://doi.org/10.2471/BLT.20.276782

García-Orosa B (2021) Disinformation, social media, bots, and astroturfing: the fourth wave of digital democracy. Profes Inform 30(6):e300603. https://doi.org/10.3145/epi.2021.nov.03

García-Vivero G, López-García X (2021) La verificación de datos en Europa. Análisis de 5 iniciativas europeas: Maldita. es, Newtral, Pagella Politica, Les Décodeurs y BBC Reality Check. adComunica: Revista Científica de Estrategias, Tendencias e Innovación en Comunicación 21:235–264. https://doi.org/10.6035/2174-0992.2021.21.12

Guzzini S (2012) The return of geopolitics in Europe?: social mechanisms and foreign policy identity crises. Cambridge University Press, Cambridge

Hallin DC, Mancini P (2004) Comparing media systems: Three models of media and politics. Cambridge University Press, Cambridge

Heiskala R, Aro J eds) (2018) Policy Design in the European Union: An Empire of Shopkeepers in the Making? Palgrave Macmillan, Cham

High-level Group on fake news and online disinformation (2018) A multi-dimensional approach to disinformation: Report of the independent high-level group. Publications Office of the European Union. https://cadmus.eui.eu/bitstream/handle/1814/70297/DeCockB_2018?sequence=1&isAllowed=y Accessed 15/07/2022

Holt K (2020) Right-wing Alternative Media. Routledge, New York

Humprecht E (2019) Where 'fake news' flourishes: a comparison across four Western democracies. Inform Commun Soc 22(13):1973–1988. https://doi.org/10.1080/1369118X.2018.1474241

Kingdon JW (1984) Agendas, Alternatives, and Public Policies. Little, Brown, Boston

López-García X, Costa-Sánchez C, Vizoso Á (2021) Journalistic fact-checking of information in pandemic: stakeholders, hoaxes, and strategies to fight disinformation during the COVID-19 crisis in Spain. Int J Environ Res Public Health 18(3):1227. https://doi.org/10.3390/ijerph18031227

Lucas E, Pomeranzev P (2016) Winning the information war. Techniques and Counterstrategies to Russian Propaganda in Central and Eastern Europe. Washington: The Center for European Policy Analysis, 1-66. https://www.semperfidelis.ro/e107_files/public/1470461530_2186_FT4490_peter_pomerantsev_edward_lucas_-_aug._2016_-_winning_the_information_war_-_the_full_report.pdf Accessed 15/07/2022

Lyons B, Mérola V, Reifler J, Stoeckel F (2020) How politics shape views toward fact-checking: evidence from six European countries. Int J Press/Politics 25(3):469–492. https://doi.org/10.1177/1940161220921732

Magallón-Rosa R (2022) De las fake news a la polarización digital. Una década de hibridación de desinformación y propaganda. Más Poder Local 50:49–65. https://doi.org/10.56151/maspoderlocal.120

Macron E (2018) Speech by Emmanuel Macron, President of the Republic at the European Parliament, Strasbourg, 17 April 2018. https://www.elysee.fr/emmanuel-macron/2018/04/17/speech-by-emmanuel-macron-president-of-the-republic-at-european-parliament.en Accessed 15/07/2022

McIntyre L (2018) Post-Truth. MIT Press, Cambridge

Merkel A (2018) Speech by Federal Chancellor Angela Merkel to the European Parliament, Strasbourg, 13 November 2018. https://www.bundesregierung.de/breg-en/news/speech-by-federal-chancellor-angela-merkel-to-the-european-parliament-strasbourg-13-november-2018-1550688 Accessed 15/07/2022

Messing S, Westwood SJ (2014) Selective exposure in the age of social media: Endorsements trump partisan source affiliation when selecting news online. Commun Res 41(8):1042–1063. https://doi.org/10.1177/0093650212466406

Meunier S, Nicolaidis K (2019) The geopoliticization of European trade and investment policy. JCMS: J Common Market Stud 57:103–113. https://doi.org/10.1111/jcms.12932

Milosevich-Juaristi M (2017) El poder de la influencia rusa: la desinformación. Real Instituto Elcano. Estudios internacionales y estratégicos, 20. https://media.realinstitutoelcano.org/wp-content/uploads/2017/01/ari7-2017-milosevichjuaristi-poder-influencia-rusa-desinformacion.pdf

Monsees L (2020) A war against truth'-understanding the fake news controversy. Crit Stud Security 8(2):116–129. https://doi.org/10.1080/21624887.2020.1763708

Montes J (2022) La desinformación: un arma moderna en tiempos de guerra. Cuadernos Periodistas 44:41–48. https://www.cuadernosdeperiodistas.com/la-desinformacion-un-arma-moderna-en-tiempos-de-guerra/

Morejón-Llamas N, Martín-Ramallal P, Micaletto-Belda J (2022) Twitter content curation as an antidote to hybrid warfare during Russia's invasion of Ukraine. Prof Inform 31(3):e310308. https://doi.org/10.3145/epi.2022.may.08
Morini M (2020) Lessons from Trump's Political Communication: How to Dominate the Media Environment. Palgrave Macmillan, Cham
Nimmo BC, François C, Eib S, Ronzaud L, Ferreira R, Hernon C, Kostelancik T (2020) Exposing secondary infektion. *Graphika*. https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf Accessed 15/07/2022
OECD (2022). Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses. OECD Policy Responses on the Impacts of the War in Ukraine. https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/ Accessed 17/12/2022
Oleart A, Bouza-García L (2019) La lutte narrative pour la signification et la politisation de « l'Europe » dans les négociations du TTIP: le récit de l'Europe bouclier contre le populisme transnational. Politique Eur 66:16–42. https://doi.org/10.3917/poeu.066.0016
Orbie J, Alcazar III ASM, Bougrea A, Nagy S, Oleart A, Paz JC, Sebhatu RW, Williams TG, Wódzka I (2023) Decolonizing rather than decentring 'Europe. Eur Foreign Affairs Rev 28(1):1–8. https://doi.org/10.54648/eerr2023001
Ördén H (2020) Deferring substance: EU policy and the information threat. In: Petersen KL, Rønn KV (eds) Intelligence on the Frontier Between State and Civil Society. Routledge, New York, p. 111–127
Ricard J, Medeiros J (2020) Using misinformation as a political weapon: COVID-19 and Bolsonaro in Brazil. Harvard Kennedy School Misinformation Review, 1(3). https://doi.org/10.37016/mr-2020-013
Rivas-de-Roca R, García-Gordillo M (2022) Understanding the European Public Sphere: a review of pending challenges in research. Eur Polit Soc 23(3):380–394. https://doi.org/10.1080/23745118.2021.188496
Rone J (2021) The return of the state? Power and legitimacy challenges to the EU's regulation of online disinformation. In: Haggart B, Tusikov N, Scholte JA (eds) Power and Authority in Internet Governance. Routledge, New York, p. 171–194
Rúas-Araújo J, Pérez-Curiel C, López-López PC (2020) New challenges and threats for journalism in the post-truth era: fact-checking and the fake news combat. In: Toural-Bran C, et al., (eds) Information visualization in the era of innovative journalism. Routledge, New York, p 154–160
Salaverría R, Buslón N, López-Pan F, León B, López-Goñi I, Erviti MC (2020) Desinformación en tiempos de pandemia: tipología de los bulos sobre la Covid-19. Prof Inform 29(3):e290315. https://doi.org/10.3145/epi.2020.may.15
Shin J, Thorson K (2017) Partisan selective sharing: the biased diffusion of fact-checking messages on social media. J Commun 67(2):233–255. https://doi.org/10.1111/jcom.12284
Stancu M (2019) Information war. case study: the role of Russia Today for coverage of the mission conducted by Russia in east Ukraine - may 2014 -february 2015. Bulletin of «Carol I» National Defence University. https://revista.unap.ro/index.php/bulletin/article/download/666/645
Szostek J (2020) What happens to public diplomacy during information war? Critical reflections on the conceptual framing of international communication. Int J Commun 14:2728–2748. https://ijoc.org/index.php/ijoc/article/view/13439/3092
The Economist (2022) The invasion of Ukraine is not the first social media war, but it is the most viral, The Economist. https://www.economist.com/international/the-invasion-of-ukraine-is-not-the-first-social-media-war-but-it-is-the-most-viral/21808456
Tuñón J, Oleart Á, Bouza-García L (2019) Actores Europeos y Desinformación: la disputa entre el factchecking, las agendas alternativas y la geopolítica. Revista Comunicación 18:245–260. https://doi.org/10.26441/RC18.2-2019-A12
Tuñón J (2021) Europa frente al Brexit, el populismo y la desinformación. Supervivencia en tiempos de fake news. Tirant lo Blanch, Valencia
Vázquez-Herrero J, Vizoso Á, López-García X (2019) Innovación tecnológica y comunicativa para combatir la desinformación: 135 experiencias para un cambio de rumbo. Profes Inform 28(3):1699–2407. https://doi.org/10.3145/epi.2019.may.01
Vizoso Á, Vaz-Álvarez M, López-García X (2021) Fighting Deepfakes: Media and Internet Giants' Converging and Diverging Strategies Against Hi-Tech Misinformation. Media Commun 9(1):291–300. https://doi.org/10.17645/mac.v9i1.3494
Wagner A, Degli-Esposti S (2022) Verdad, desinformación y verificación: contexto de estudio y contribución al debate. Dilemata 38:5–12. https://www.dilemata.net/revista/index.php/dilemata/article/view/412000503
Waisbord S (2018) Truth is what happens to news: on journalism, fake news, and post-truth. Journal Stud 19(13):1866–1878. https://doi.org/10.1080/1461670X.2018.1492881
Wagnsson C, Hellman M (2018) Normative power Europe caving in? EU under pressure of Russian information warfare. JCMS: J Common Market Stud 56(5):1161–1177. https://doi.org/10.1111/jcms.12726
Williams BA, Delli Carpini MX (2011) After broadcast news: Media regimes, democracy, and the new information environment. Cambridge University Press, Cambridge
Wæver O (1995) Securitization and desecuritization. In Lipschutz R (ed) On Security. Columbia University Press, New York, p 46–86

## Acknowledgements

The authors acknowledge the support of the following research projects: AICO/2021/063 funded by Generalitat Valenciana; RED2022-134652-T funded by MCIN/AEI/10.13039/501100011033/; Ref: 101126821-JMO-2023-MODULE (DISEDER-EU) and Ref: 101083334-JMO-2022-CHAIR (FUTEUDISPAN), both funded by the Education, Audiovisual and Culture Executive Agency (EACEA), belonging to the European Commission; and Grant Agreement nr. 101061330 (RECLAIM) funded by the Horizon Europe. However, the content of this article is the sole responsibility of the authors and reflects only their views. Any funder (Generalitat Valenciana, AEI, EACEA, European Comission and European Union) cannot be held responsible for any use which may be made of the information contained therein.

## Author Contributions

Conceptualization, AC-R, JT, and LB-G; writing—original draft preparation, AC-R, JT, LB-G; writing—review and editing, JT, and LB-G; supervision, AC-R, JT, and LB-G; project administration, AC-R; funding acquisition, AC-R. All authors have read and agreed to the published version of the manuscript.

## Competing interests

The authors declare no competing interests.

## Ethical approval

This article does not contain any studies with human participants performed by any of the authors.

## Informed consent

This article does not contain any studies with human participants performed by any of the authors.

## Additional information

**Correspondence** and requests for materials should be addressed to Andreu Casero-Ripollés.