



D6.7 Safeguarding Liberal Democracy in the Digital Age: Multiple Principles of Internal and External Policies on Countering Foreign Information Manipulation and Interference and Building Digital Sovereignty

Jonáš Srovátka, Faris Kočan, Anđela Đorđević, Marko Hočevar, Jan Daniel

Table of Contents

<i>Abstract</i>	2
<i>Introduction</i>	3
<i>Theoretical background</i>	3
<i>Note on methodology</i>	5
<i>Multiple fights against disinformation in the EU</i>	7
Disinformation, FIMI, Influence operations: A note on multiplicity of terminology	8
<i>3Ds: organising principles of the EU polices on disinformation</i>	10
Organising principle “Defend”	11
Organising principle “Direct”	12
Organising principle “Delegate”	13
Summary: Towards comprehensive digital sovereignty	13
<i>Strategic Contestation and Digital Sovereignty in the Western Balkans: The EU's Approach Towards the Region at a Crossroads</i>	14
The FIMI challenge in the Western Balkans and the European response	15
Digital Strategies and Information Governance on the national level	16
Sovereignty deficiencies amid emerging digital multipolarity	19
Digital dependency, tech integration and FIMI	20
EU’s digital sovereignty projection	21
Digital Silk Road? China’s role in the Western Balkans	22
American response: Clean Network Initiative	23
Conceptual Reflections: Ontological Security and Assemblage Perspective as determinants of the Western Balkans' digital policies	24
Summary: Digital politics between identity-seeking and fragmented assemblages	25
<i>Conclusions and policy recommendations</i>	26
<i>References</i>	28

Abstract

This report examines the European Union's approach to managing disinformation and establishing digital sovereignty in response to trans-local information threats. The analysis evaluates the organising principles underlying the EU's approach, which seeks to control disinformation circulation while preserving liberal democratic values in an increasingly competitive geopolitical environment. The report focuses on two primary dimensions: internal EU-level developments in the area of control over the information sphere and the extension of European digital governance to the Western Balkans. It outlines the three main organising principles guiding the EU's policies in this area – Defence, Direct, and Delegate - and points out how they complement each other, but might also clash if used incoherently. The second part of the report then extends the analysis to the Western Balkans and unpacks the European efforts guided by these logics in an environment marked by geopolitical competition and structural technological dependency of regional states. The analysis concludes with practical recommendations for strengthening European policies against FIMI both within EU borders and in neighbouring regions, while maintaining commitment to liberal democratic principles essential for the EU's role in contemporary global governance.

Introduction

The report concludes the research performed in Work Package 6 (WP6) and evaluates the EU's attempts to manage trans-local production and circulation of (dis)information in online space—the new plane of international politics. More specifically, this report unpacks the different organising principles on which the broad EU's approach to managing disinformation and controlling the digital information space, an agenda which came to be known as the European Digital Sovereignty (Falkner et al., 2024), is based. The second part of the report looks beyond the EU to its neighbourhood. It considers the interplay of the EU's attempts to control the digital space beyond the EU borders with multiple other national and international attempts aimed at building digital sovereignty. Doing so, the report builds on the theoretical framework developed and refined in the previous deliverables in the Work Package (Ditrych, 2024; Ditrych et al, 2025; Kratochvíl et al., 2025), other conceptual and empirical studies carried out in the project (Bouza García & Oleart, 2023; Conrad, 2025; Casero-Ripollés et al., 2023; Proto et al., 2025), as well as analysis of the relevant EU documents and secondary literature.

The report considers the European digital agenda broadly and focuses both on the development at the EU level and the extension of European digital governance to the Western Balkans in order to understand how the EU seeks to react to the problem of disinformation and its trans-local nature. In this respect, we further develop our previous observations, which highlight the diffused nature of disinformation assemblage, which brings together territorially uncoupled human and non-human actors and actants, including the foreign producers of disinformation, online audiences in the EU member states and beyond, as well as technologies, infrastructures and platforms which provide the material underpinnings of the new, boundless, digital space (Ditrych et al., 2025). In this respect and on the broader level, the report contributes to understanding how the EU seeks to safeguard its public sphere and control its digital sphere, as an essential condition for the preservation of liberal democracy, in an increasingly competitive geopolitical environment, where European adversaries make use of the information sphere to influence European population (Conrad, 2025; Ditrych et al., 2025; Kratochvíl et al., 2025). Considering this goal inside the EU and in its neighbourhood is essential for understanding the role of the EU in the present global order.

The report is structured as follows: It first introduces the conceptual and methodological toolbox and explains its connection with the rest of the work package. It then proceeds to unpack the organising principles of the EU's struggle against disinformation and FIMI as part of broader efforts aimed at developing digital sovereignty. The third section moves its attention to the European neighbourhood, more specifically the Western Balkans, to understand the interplay of different attempts to build digital sovereignty. The report's conclusion provides practical recommendations to strengthen European FIMI and digital policies both on the EU level and in the neighbourhood while safeguarding their liberal values.

Theoretical background

In this report, we combine several theoretical approaches utilised in the previous reports to capture different dimensions of policies aimed at countering disinformation, protecting the liberal public sphere, and countering FIMI. Namely, we combine the Ontological Security Theory with an Assemblage Theory and focus on organising principles that give particular policy assemblages their strategic direction.

Ontological Security Theory (OST), originally articulated by Giddens (1991), refers to the confidence that individuals or collectives have in the continuity of their self-identity and their surrounding social and material environments. In International Relations, this has been further developed by scholars such as Mitzen (2006), Steele (2008), and Kinnvall (2004), who argue that states, like individuals, seek ontological security through routines, narratives, and reliable relationships. This includes alliances, institutional affiliations, and policy trajectories that provide existential reassurance and predictability. In this report, we use the ontological security theory primarily to illuminate the practices that the EU uses to restore the inside/outside boundaries and reestablish the stable sense of self in the face of ontological insecurity brought by the destabilisation of the international liberal order, epistemic order based on it, and the rise of attention to FIMI and its impact on the liberal democracies (see Adler & Drieschova, 2021; Ditrych, 2025). In the context of the WB, explored in the second part of this report, OST concerns are especially salient given the region's history of state disintegration, contested sovereignty, and prolonged transitional uncertainty. States such as Kosovo and BiH experience chronic anxiety over their international recognition, territorial integrity, and domestic cohesion. Digital policy is not merely a matter of infrastructure or economic development for these states. It is deeply tied to identity formation and state legitimacy.

To account for the institutional and material complexity of facing FIMI, OST benefits from being complemented by assemblage thinking. Assemblage theory, developed by Deleuze and Guattari (1987) and elaborated in IR by scholars such as Barry (2013), Acuto and Curtis (2014), and Müller (2015), conceptualises governance and power as emergent from the interactions of diverse elements: human and non-human, material and discursive, global and local. Other scholars (de Goede & Simon, 2013) then refine this perspective and propose to focus on assemblage mostly in terms of how certain policies are put together, linking a particular articulation of the problem with multiple responses. In the previous Reclaim reports, we made use of assemblage theory primarily to capture the trans-local nature of foreign interference assemblage with its connections between foreign powers and local actors who, for various reasons, accept and further spread disinformation (Ditrych et al., 2025). Here, we focus on reactions to disinformation and unpack the multiple logics of the European and national policies of countering FIMI as ways of stabilising the digital borderscape and reclaiming control in the digital sphere (see Ditrych, 2025). As De Goede and Simon (2013, p. 317) state with regard to assemblage analysis in the context of the European policies aimed at governing radicalism, this approach allows for “*render(ing) visible and conceptualis(ing) the 'reach' of the EU*” in a particular policy field. The assemblage of different actors, practices, and discourses coheres around particular threat representation and responses to ontological insecurity while combining elements of both European and national policies.

We capture the strategic directions around which particular assemblages cohere by outlining different organising principles developed in the EU's policies of countering FIMI, thus building the EU's digital sovereignty in recent years. By organising principles, we mean the combination of a particular framing of FIMI and disinformation as a problem to be governed and reacted to, which has its roots in different parts of the European institutions (de Goede & Simon, 2013), but which also stems from a particular feeling of ontological insecurity. The attention to organising principles, together with assemblages, allows us to combine the attention to the “problem” and “logic” which makes particular reactions apparent, with the multiplicity of actual practices through which it is put into practice. However, the assemblage perspective also helps us to go beyond the imaginary of the organising principles as separate boxes. Instead, we propose the image of

intertwined circles overlapping in some parts and not in others, as some instruments and actors are enrolled in multiple assemblages simultaneously.

In the first part of the report, we foreground the European level and develop the organising principles based on the key EU documents on FIMI and countering disinformation. While the focus here is narrowly on disinformation and FIMI (more on the terminology below), we understand it as a part of an effort to establish European control over the digital (information) space and set up a series of Europe-wide rules, which ultimately support the idea of European digital sovereignty (Falkner et al., 2024; Flonk et al., 2024). In the second part of the report, we focus instead on the national level in the Western Balkan states and how European attempts to counter FIMI and build digital sovereignty beyond the physical and digital EU borderspace (see Carver, 2024) interact with national policies aimed at establishing digital sovereignty in informational and technological areas.

Note on methodology

Our methodological approach treats disinformation less as an empirical “problem to be solved” and more as an entry point into understanding how political orders manage insecurity and project authority in fragmented digital environments. Rather than measuring disinformation flows or fact-checking their veracity, we analyse how disinformation is framed, mobilised, and institutionalised within European Commission (EC) policy documents and Western Balkan (WB) digital strategies. This approach allows us to study policies aimed at countering disinformation and foreign interference and building digital sovereignty as both a constitutive narrative practice – through which actors articulate boundaries of self and other – and as a governance object that enrolls infrastructures, regulations, and societal actors into wider assemblages (Ditrych, 2025).

Our analysis in the first part of this report is limited to EC and the policy documents written in its name. However, we know that multiple other actors are involved in creating EU policies towards disinformation. On the institutional level, the European Parliament articulates political demand for addressing the problem. Particularly relevant in this respect were the Special Committee for foreign interference in all democratic processes in the EU, including disinformation (INGE) and the Special Committee on the European Democracy Shield (EUDS). The debate on the issue in the broader “Brussels bubble” was facilitated by an assemblage of think-tanks, activists, researchers and lobbyists who helped to shape the thinking and approach of EC bureaucrats (see Cesaro-Ripollés et al., 2023 ; Datzler & Lonardo, 2023; Ördén, 2019).

The analysis is guided by two interlocking conceptual frameworks linked by the notion of organising principles. Ontological Security Theory directs attention to how EU institutions and WB states seek existential reassurance in the face of perceived instability, treating disinformation as a threat to coherent identity and narrative continuity. As such, it animates and orients the particular organising principles. Assemblage thinking, in turn, highlights the heterogeneous, multi-scalar configurations through which disinformation is governed, spanning bureaucracies, digital infrastructures, civil society actors, and global platforms. As we noted previously, the assemblages cohere around particular organising principles as these give the assemblages a sense of strategic direction. Taken together, these perspectives foreground how counter-disinformation measures are not simply reactive, but when put in place, they also reaffirm certain readings of the problem and hence, become productive of new realities.

Methodologically, this conceptual perspective results in a mixed strategy combining different data and ways of analysing them. On the European level, it means reading policy texts and strategies for their explicit content and the underlying logic of the organisation. The principles distilled from EU documents serve as heuristic devices to identify how disinformation is positioned as a security threat, a regulatory challenge, or a societal responsibility. Our research is based on documents presented on the EC’s website that are related to the topic of disinformation (European Commission n.d.-a). In this respect, we do not differentiate between different parts of the EC; rather, we are interested in which principles the EC stands behind as a whole.

Our analysis focuses on documents and institutional mechanisms presented by the EC related to disinformation and relates them to the project’s theoretical framework. We decided to start in 2018, when the Action Plan against Disinformation was published. The number of relevant documents and initiatives increased significantly in the following years. To understand the way in which terms are used in EU documents and how, it is crucial to set an effective research strategy. For instance, focusing only on term FIMI would be too reductive as it would limit the research to documents dealing with foreign interference. This would obscure the ambition to describe the multiplicity of organising principles used to understand the phenomena and enact a multiplicity of responses. Therefore, we did not orient our analysis around specific keywords but decided to focus on a set of documents that EC itself presents as being related to the topic of disinformation, even though each of them understands it slightly differently. As the term “disinformation” remains the most frequent in analysed documents, we also use it in the text as an umbrella term for all other concepts used to describe the phenomena.

Table 1. List of relevant documents and institutional mechanisms reviewed

Year	Name
2018	Action plan against disinformation
	Code of Practice against Disinformation
2019	The Rapid Alert System is established
2020	European Digital Media Observatory is launched
	European Democracy Action Plan
	Proposal for the Digital Services Act
2022	Strengthened Code of Practice on Disinformation
	Proposal for the European Media Freedom Act
2023	Defence of Democracy Package
2024	Regulation on the transparency and targeting of political advertising
	Artificial Intelligence (AI) Act
	Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness

In other words, the analysis reflects how the EC presents its actions against disinformation and which underlying principles these actions are based on. We do not aim to provide a critical evaluation of the level of fulfilment of presented policies in practice or contemplate their utility or potential adverse side effects. We aim to present different organising principles that guide the struggle against disinformation and FIMI, as well as the logic of counter-measures on which these are based. In the Western Balkans context, we supplement this

document analysis with secondary literature and regional case material to explore how these organising logics intersect with local vulnerabilities, external influences, and contested sovereignties. By privileging conceptual abstraction over empirical measurement, the study aims to capture the structural and narrative dimensions of disinformation as central to the politics of digital sovereignty in Europe's periphery.

Multiple fights against disinformation in the EU

The European Union (EU) started focusing on disinformation in 2015 in response to Russian information operations. At that time, the topic was perceived strictly through security lenses, and it remained confined to offices of the European External Action Service (EEAS) and oriented toward threats coming from abroad. A decade later, the situation changed completely. The issue of disinformation spilt over to multiple areas of the European Commission's (EC) interest and is related to different policies such as regulating social media, political advertisement, and education. Research conducted in Reclaim previously highlighted the evolution of the European institutional structures (Navarro et al., 2025; Proto et al., 2025) and their differing logics (Casero-Ripollés et al., 2023; García-Gutián, 2024) as well as crises that brought the disinformation challenge to the public spotlight of different European states (Ditrych et al., 2025), or the initiatives in the area of journalism (Bouza et al., 2025). A combination of internal bureaucratic development and real-world crises can partially explain the rapid proliferation of the countering disinformation agenda and its expansion.

However, this is only part of the story. The findings of our analysis are that despite the topic of disinformation spreading into multiple areas, the main organising principles of perspective on the problem remain fairly similar since 2018. In that year EC published its Action Plan against Disinformation in which it outlined four main pillars of the response to the problem – “improving the capabilities of Union institutions to detect, analyse and expose disinformation”, “strengthening coordinated and joint responses to disinformation”, “mobilising private sector to tackle disinformation” and “raising awareness and improving societal resilience” (European Commission 2018a). After reviewing EC's reports, strategies and other documents published since, we argue that these organising principles remain consistently present in different strands of activities taken by the EU in countering disinformation and FIMI more broadly.

We suggest categorising the EU's approach to the topic according to what we call the 3Ds model of organising principles. These correspond not only to how the problem of disinformation is perceived, but also, referring to our central conceptual apparatus, to how the EU assembles diverse tools and policies as coping devices for ontological insecurity to respond to fragmentation and decay in the international normative order (Ditrych, 2025). The first principle is to *Defend* perceiving disinformation as a security threat from abroad that has to be exposed and prevented. Here, the EU reinforces its geopolitical and value-based identity, while drawing a strict line (a border-scape, see Ditrych, 2025; Ördén & Pamment, 2021; Hedling & Ördén, 2025) between the acceptable and unacceptable, between the inside and outside information actors (see also Proto et al., 2025). The second principle is *Direct*. This principle stems from understanding the spread of disinformation and its impact on the public sphere as a by-product of the development of digital information space (social media in particular). As such, it performs instead the market-based and regulatory side of the EU (see also Bouza García & Oleart, 2023) as a response to the ontological and epistemological insecurity. In this respect, the *Direct* assemblage relies on tools that aim to force the market players to increase transparency and accountability, and by doing so, they are enrolled into the assemblage as key actors responsible for managing the borderscape. According to this principle, the platforms themselves would help to keep the unwanted actors

out, acting upon the directions of the EU and protecting its identity and public sphere. The third principle, which we call *Delegate*, is focused on actors outside of EC bureaucratic structures and aims to empower local non-market actors - fact-checkers, journalists, researchers or teachers. This extends to the assemblage of the area of society at large through reaching out to information professionals, who are supposed to tackle problems in their respective environment and area of expertise (García-Gordillo et al., 2025). This principle upholds the liberal identity of the EU in the face of ontological insecurity.

We are not the first to aspire to categorise the EU's different approaches to the topic of disinformation. Jurás (2024) emphasises the security-minded nature of the EU approach and suggests analysing its policies through the prism of militant democracy. According to her categorisation, these measures should be either restrictive – taking active steps to counter disinformation – or inclusive, building institutional and societal resilience. We certainly agree that the original relation of the topic of disinformation with debates on security needs to be taken into account. However, we believe the securitisation perspective alone does not adequately capture how the topic got established in many EU policies.

Casero-Ripollés, Tuñón and Bouza-García (2023), similarly to Ördén (2019), suggest the existence of two different approaches – geopolitical and regulatory – that the EU takes when responding to disinformation. The authors present these approaches as opposing, which leads to dissonance in measures promoted by European institutions. While these articles inspired our thinking about the organising principle of EU policies on disinformation, these studies should be pushed further to account for the wider counter-disinformation and counter-FIMI ecosystem connected to the EU institutions. The authors limit their focus to the European institutions and therefore omit partnerships established with civil society that are in practice an inseparable part of the counter-disinformation assemblage. Given the messy and fragmented nature of policy-making and the dynamic of the topic, we should not limit ourselves to an “either/or” binary.

Complex bureaucratic structures are improbable to produce only one coherent policy response to a complex societal problem. Instead, given by spillover of topic to multiple institutions with particular agendas and understandings, their response is expected to be multifaceted, sometimes complementing and sometimes contradicting each other. Producing contradictory policy outcomes is a bug and a feature of complex bureaucratic structures such as the EU. We believe that the perspective put forward in this study, which forefronts the combination of assemblage and organising principle around which it coheres, enables us to provide a more nuanced picture.

[Disinformation, FIMI, Influence operations: A note on multiplicity of terminology](#)

In the past decade, the EC documents have used multiple terms to label and manipulate falsehoods in the online space. To a certain degree, these terms represent the different organising logics outlined above and reflect the diverse understandings of the disinformation problem and its origins. At the same time, this terminological confusion reflects the many origins of the disinformation agenda.

According to the EC's narrative, the disinformation agenda took a specific shape for the first time in 2015 when a task force was established to prepare a plan for strategic communication. The task force's activity aimed to respond to “to challenge Russia's ongoing disinformation campaigns” (EUvsDisinfo, 2023a). Following the *Defend* logic, this effort resulted in establishing the East Stratcom Task Force, which is mandated to monitor, expose, and analyse Russian information operations in EU member states and their close neighbours. The security-centred perspective was reinforced by another document approved in 2016,

the Joint Framework on Countering Hybrid Threats, which, among other things, suggested increasing coordination with NATO (European Commission, 2016).

The Action Plan against Disinformation presented in 2018 was a significant departure from this perspective, as it significantly broadened the area of counter-disinformation activities. The document suggested that defence against disinformation should stay on four main pillars– *“improving the capabilities of the Union institutions to detect, analyse and expose disinformation”*, *“strengthening coordinated and joint responses to disinformation”*, *“mobilising the private sector to tackle disinformation”* and *“raising awareness and improving societal resilience”* (European Commission 2018a). On the one hand, a combination of multiple approaches is entirely understandable, as disinformation presents a multifaceted social phenomenon requiring various policy solutions. However, it also shows the differing organising logics stemming from different conceptions of the EU, its role in managing the borderscape and its ontological security. A similar mixture of different logics is observable in multiple broader security-oriented documents, such as the recent document Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness (European Commission, 2024). This document explicitly connects the different organising logics enshrined in the reviewed documents, while arguing for enhancing preparedness by reaching out to civil society, strengthening the ability to deter disinformation threats by potential punishment and stresses the obligations of platforms in managing the borderscape in the information sphere.

As the interest in the topic started to emerge in different parts of the EC (see Casero-Ripollés et al., 2023; Datzer & Lonardo, 2023), the term’s meaning started to stretch to fit into new policy areas. The Action Plan 2018 defines disinformation as *“verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm”* (European Commission, 2018a). Already, this definition hints at the fact that the original focus on information operations from abroad starts to shift as messages causing *“public harm”* or disseminated for *“economic gain”* can be spread by a wide variety of actors.

Communication on the European Democracy Action Plan from 2020 further stretches the meaning of the term since it claims that it is necessary to *“distinguish between different phenomena that are commonly referred to as ‘disinformation’”*. The documents list four different phenomena that should be addressed: misinformation, disinformation, information influence operation, and foreign interference in the information space. This broader definition of the problem allows for the promotion of a wider set of policy responses, as shown in the document (EUR-lex, 2020).

Since 2021, the EEAS has adopted the concept of Foreign Information Manipulation and Interference (FIMI), which it presented as synonymous with disinformation (for detailed discussion see Proto et al., 2025). However, the perspective differs quite significantly from the previous understanding of the term (offered for instance by Action Plan from 2018) as FIMI was defined as *“a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory”* (European External Action Service, 2022). According to this perspective, EEAS focuses not on individual pieces of false information but on a wide range of coordinated activities conducted by malign actors. While part of this adaptation of vocabulary certainly has been motivated by reflection of realities of information operations, its logic has to do

also with internal bureaucratic process as individual tried to define (and by doing so protect) their specific role in countering disinformation.

The multiplicity of terms referring to the phenomenon – disinformation, FIMI, information manipulations – was used to a certain extent interchangeably in the EC documents. The prime example is the EC website itself. The general section Topic providing a signpost to different EU policies uses the term “*Disinformation*” (European Commission, n.d.-b). However, the linked websites presenting the EU approach in more detail are titled “*Strategic communication and countering foreign information manipulation and interference*”, and in the text terms “FIMI” and “disinformation” are used to a certain extent interchangeably (European Commission, n.d.-a). We want to point out that this observation is not a necessary criticism of the lack of consistency in the vocabulary of the EC institutional bodies. Instead, we perceive the existence of multiple vocabularies as a manifestation of multiple organising principles that emphasise different perspectives on the issues and multiplicity of reactions.

Nevertheless, the issue gets even more complicated as the notions of disinformation and FIMI started to be mentioned in only tangentially related agendas. This can be illustrated by the Regulation on the transparency and targeting of political advertising that entered into force in April 2024. In the first chapter of the document, its necessity is explained (among other things) by risks related to disinformation (EUR-Lex, 2024). At the same time, it remains relatively unclear how this specific piece of legislation will address the issue. A similar case is the Artificial Intelligence Act adopted in August 2024, which mentions disinformation in passing but does not further elaborate on how the new regulation will address them (European Commission n.d.-c). Nevertheless, these documents are presented by the EC as a contribution to fighting against disinformation.

To clarify our argument, we do not claim that the analysed documents do not help to react to some of the challenges related to disinformation. However, we argue that the term disinformation is not even mentioned in these documents, which demonstrates how this topic proliferated into various EU policies and highlights the multiplicity of assemblages at play. Considering this situation, the need to distinguish different organising principles is even more evident.

3Ds: organising principles of the EU policies on disinformation

When defining the organising principle of the EU policies against disinformation, we found it helpful to be inspired by the pillars presented in the Action Plan in 2018. It is quite remarkable that the suggested approaches remain fairly recognisable across the analysed documents. As outlined above, we distinguish three organising principles of the EU policies:

- *Defend* – policies perceiving disinformation as a security threat from abroad that has to be exposed and prevented
- *Direct* – policies understanding of the spread of disinformation as a by-product of the development of digital information space (social media in particular), and trying to solve it through regulation that increases transparency and accountability
- *Delegate* – policies aiming to engage actors outside of EC bureaucratic structures and aims to empower them – fact-checkers, journalists, researchers or teachers – to tackle problems in their local environments

We do not treat these organising principles as mutually exclusive and should not be perceived as separate. Instead, we see them as coexisting within the complex body of the EC's institutions, similarly to how they exist in different ways on the national levels (see Ditych et al., 2025). Depending on the institution, policy, and broader assemblages in which these are enrolled, they might overlap and complement each other as they are all linked to the broader idea of establishing sovereign control over the digital information space. To illustrate our thinking on an example, for instance, an institutional actor whose tools and thinking about the problem correspond primarily to the *Defend* principle still needs a set of rules and regulations clarifying the conditions of removal of the bot network from social platforms. At the same time, the actor might not eliminate the possibility of engaging with researchers outside of EC institutions. Similarly, policies informed by the *Delegate* principle can still be shaped by a security-centred mindset or used to oversee rules imposed, for instance, on social media. Therefore, our categorisation operates only on higher levels of abstraction, and the dynamics of individual situations should be analysed on a case-by-case basis.

This returns us to the trans-local nature of the responses to disinformation, which might have a strategic direction set at the centre but are often also taken up by a multitude of local initiatives. The three organising principles are thus not strictly divided or opposing, but instead overlap and intertwine depending on the specific policy and the particular assemblage where they are put into practice. The reason why these different perspectives can be in dialogue is that they ultimately serve the same purpose, which is the development of the EU's digital sovereignty as an aspirational coping mechanism with the perceived ontological insecurity and a series of crises coupled with a more confrontational international environment that has hit the EU since 2014 (Ditych et al., 2025).

While one can reasonably doubt that the authors of the Action Plan from 2018 had this goal in mind, the changing nature of international politics forced the EU decision-makers to put the problem of disinformation into a much broader perspective of policy towards digital space in general and ultimately building the European digital sovereignty (see Flonk et al., 2024). We are convinced that this is also why the issue of disinformation has become prominent in the EU's agenda. It does not stand only for the malicious actions of specific outside actors. However, it represents the spearhead of efforts to bring order and sovereign control into the wilderness of the digital plane – undoubtedly one of the most significant tasks for any political structure in the 21st century – and react to ontological and epistemological insecurities felt across the EU and its member states. Insecurities that do not stem only from the actions of foreign competitors and proliferation of disinformation and misinformation in digital space, but also from the profound technological and political changes in the EU itself and from the wider crises of the international liberal order.

Organising principle “Defend”

The organising principle Defend is the oldest of approaches used by EU institutions to conceptualise the problem of disinformation. In this view, the main challenge is hostile information operations of malign actors – Russia and China in particular. As already explained in relation to the term FIMI, EU defence should not be limited to falsehoods. However, it should focus on a wider set of organised, manipulative activities targeting not only the information sphere but also the digital and other infrastructures and institutions at large. Also, the list of actors against which the EU's information space should be defended remains vaguely defined. This is exemplified by a statement on EEAS websites claiming that its role is to assist EU civilian and military missions targeted by FIMI (European External Action Service 2025a). This – from an operational standpoint, obviously

completely understandable – approach suggests that the EEAS remit can be flexibly adjusted and so could be the assemblage through which it is done.

The key institutional representative guided by the *Defend* principle is EEAS, whose team, East Stracom Task Force, has focused on Russian information operations since 2015. This team operates a website, EUvsDisinfo, collecting case studies, providing analysis and raising public awareness about the issue. The other analytical product organised according to the *Defend* principle is EEAS Reports on Foreign Information Manipulation and Interference Threats, published on a yearly basis (European External Action Service 2025b). At the same time, the conceptual framework EU FIMI Toolbox presented in 2025 shows how *Defend* organising principle intertwines with other principles and, in line with “*whole-of-society approach*”, emphasises the need to combine security measures with resilience building and regulation (European External Action Service 2025a).

Up to this point, the most notable manifestation of the Defence organising principle was sanctions on Kremlin-affiliated outlets perceived as “*essential and instrumental in supporting Russia’s aggression against Ukraine*” in 2022. The decision was made since these information sources were evaluated as significant and directly threatening the EU’s public order and security (European Commission n.d.-d). While the specificity of the condition related to the Russian invasion of Ukraine is hard to overstate, it should be noted that such a formulation suggests that sanctioning as a tool against spreaders of disinformation could be used again in future.

Organising principle “Direct”

According to the organising principle *Direct*, the spread of disinformation is a feature of an unregulated online information environment – social media in particular. Therefore, the right answer to the problem is to set and enforce rules according to which it is organised. Disinformation is only one of many problematic phenomena (others being hate speech, fraud, copyright infringements, etc.), reinforced by a lack of regulatory oversight of the digital information space. That is why the emergence of the organising principle *Direct* should not be understood as a response to the threat of disinformation per se. Instead, disinformation has been established as a significant problem that can also be seen through the lenses of the *Direct* organising principle.

The first introduction of the organising principle *Direct* into the topic of disinformation, occurred in 2018 when the EC presented the Code of Practice on Disinformation to which social media companies could voluntarily subscribe. The Code (updated in 2022) steps, such as demonetising disinformation spreaders, strengthen the measures to reduce manipulative behaviour used to spread disinformation (such as fake accounts or bot networks) or empower users who could, through enhanced tools, recognise, understand, and flag disinformation (European Commission n.d.-e).

The game-changing moment was the adoption of the Digital Services Act (DSA) in August 2023. This co-regulatory framework established a binding mechanism that would allow oversight and evaluate social networks’ ability to ensure a safe environment for their users, including specific commitments related to the prevention of illegal and harmful activities (including disinformation) (European Commission n.d.-e). The legal framework also made it possible to punish for non-compliance, and currently, the EC has launched formal proceedings against several large online platforms, including X, TikTok, Facebook and Instagram. In February 2025, EC and the European Board for Digital Services endorsed the integration of the 2022 Code of Practice

into DSA, which signals that they aim to use this legislation to enhance regulatory policies against disinformation (European Commission n.d.-f).

Organising principle “Delegate”

While the previous two organising principles are predominantly inward-looking and focused measures taken by the EC institutions, the organising principle *Delegate* aims to empower civil society to deal with the problem of disinformation. Its approach centred on citizens and their empowerment to solve community problems aligned with the concept of “whole-of-society approach” to threats to security and safety. The specific tactics within this organising principle differ and include education, fact-checking, and research, but their underlying logic is that the EC delegates responsibility to address disinformation to local actors who have the best expertise in a given area or context.

The elements of the Delegate organising principle were presented already in the beginning of shaping policies against disinformation since the EEAS actively encourages civil society and researchers to contribute to the website EUvsDisinfo with case studies of Russian disinformation from their countries. However, the serious start of delegating responsibilities occurred in 2020 when the EC funded the establishment of the European Digital Media Observatory – a network of hubs gathering researchers and fact-checkers in member states. According to publicly available information, the EU funded 45 projects focusing on disinformation at the time of writing, focusing on such different topics as the use of AI in support of citizens to verify information, promoting information literacy in schools or researching the tactic of information suppression as the FIMI technique (European Commission n.d.-g).

Summary: Towards comprehensive digital sovereignty

The profound reshaping of information space, combined with the restructuring of the international order, leads to a crisis, causing anxieties in societies. These challenges force states, governments, and international institutions to search for new ways to manage ontological security. As the nature of the challenge is multifaceted, a single-minded approach (such as the securitisation of manipulative statements circulating in the information space) is deemed to fail. At the same time, the contradictory nature of some policies and thinking about FIMI and disinformation might lead to mutually clashing interpretations and practices on the ground.

The need for a broader perspective is visible in the EU’s approach, which might start with measures guided by the organising principle *Defend*, aiming to counter information operations from Russia. However, only a few years later, it became clear that this perspective is not sufficient and has to be complemented – especially in a democratic setting – with ambition to set clear rules for the main actors of the digital information environment (organising principle *Direct*) and engagement with civil society (organising principle *Delegate*). In this holistic approach, the topic of FIMI loses its predominance and becomes only one of many features of the new information space that needs to be tackled. Therefore, EU policies associated with addressing disinformation might seem unrelated or even contradictory.

We argue that this is only partially a problem, as the analysis must focus not on a single policy but should consider the broader underlying ambition to provide ontological security in a changing world and the multiplicity of the initiatives pursued in the name of establishing control over the digital information sphere. Following previous research (Flonk et al., 2024), we propose to frame these efforts as an ambition to define digital sovereignty in the EU context in opposition to the way in which digital information space is approached

by other great powers – the United States, Russia and China. The EU's ability to define its unique vision and promote rules upholding it will indicate its ability to be a relevant actor in international politics in the multipolar order of the 21st century. In the second part of this report, we thus turn to the competition over different aspects of digital sovereignty in the European neighbourhood, more specifically in the Western Balkans.

Strategic Contestation and Digital Sovereignty in the Western Balkans: The EU's Approach Towards the Region at a Crossroads

If the previous part of this report aimed to sketch the primary organising principles of the EU's approach to disinformation and FIMI, it should be noted that these did not concern only the territory of the EU member states, but also the EU's neighbourhood. In this study, we focus specifically on the Western Balkans and how the EU and national governments seek to manage the ontological insecurity and digital borderscape in this region.

The Western Balkans (WB) has long represented a geopolitical fault line and a normative test for the European Union. Historically regarded as the “powder keg of Europe” due to its multiethnic composition underpinned by nationalisms and political instability (Larrabee, 1994, p. 11), the region underwent a dramatic rupture with the violent disintegration of Yugoslavia in the 1990s. The wars that accompanied this process, compounded by the fall of socialism, revealed the fragile foundations of peace and security in the region, opening the space for a potential transformation toward European integration (Zartman, 2005, p. 138). Following the wars, the EU constructed a new strategy for the WB grounded in economic assistance, normative engagement, and integration incentives (Rupnik, 2011, p. 4). This approach gained structure through initiatives such as the Stability Pact for South-Eastern Europe, launched in 1999 to foster peace, democracy, and human rights; and the Stabilisation and Association Process, formalized in 2000 to provide a roadmap for eventual EU membership through conditionality on governance reforms, rule of law, and economic liberalization (European Commission, 2003; Blockmans, 2004, p. 310). While Croatia's accession to the EU in 2013 was presented as a “catalyst and reference point” for the region (European Commission, 2011, p. 2), the overall enlargement process has stagnated. Scholars have argued that the EU's transformative power in the region has been constrained by internal EU crises, ambiguous membership commitments, and the limited statehood of candidate countries (Elbasani, 2013; Barbulescu & Troncota, 2012, p. 103; Börzel, 2011, p. 14). The phenomenon of “shallow Europeanisation” has thus come to define much of the region's recent experience (Noutcheva, 2009, p. 165). This strategic ambiguity has stalled the EU's transformative leverage and created fertile ground for external influence and disinformation. Weak institutions, contested sovereignties, and uncertain accession timelines have turned information spaces into key arenas of struggle, where domestic elites and foreign powers alike compete to shape narratives and legitimacy.

This section unfolds in three steps: it first situates the Western Balkans within the EU's broader enlargement trajectory and the vulnerabilities that have enabled disinformation to flourish; it then traces how external actors such as Russia and China, together with domestic elites, instrumentalize disinformation to advance strategic and political goals; finally, it shows how these dynamics intersect with the EU's own counter-disinformation logics and broader digital sovereignty agenda. To capture this complexity, it is necessary to look

simultaneously at the role of states, great powers, and the EU: states because their institutional weaknesses and identity politics shape the local uptake of disinformation; great powers because they project competing technological models and narratives into the region; and the EU because it remains both a normative anchor and a source of strategic ambiguity. Only by integrating these levels can we see how disinformation both reflects and reshapes the contested sovereignty of the Western Balkans.

The FIMI challenge in the Western Balkans and the European response

Disinformation in the WB is not merely a by-product of poor media regulation but a deliberate strategy aimed at eroding public trust, exacerbating ethnic divides, and undermining pro-European reform coalitions (Freedom House, 2022). Russian disinformation efforts have been particularly sustained, using both traditional media and digital platforms to propagate anti-EU and anti-NATO narratives, often aligned with local nationalist discourses (BIRN, 2023; EUvsDisinfo, 2023b; CHS, 2022). In Serbia, pro-Kremlin messaging exploits historical, religious, and cultural affiliations, with narratives portraying Russia as a reliable partner and the EU as an unreliable and biased actor (CIDOB, 2023). In BiH, disinformation exploits constitutional fragmentation and ethnic competition, frequently targeting the state's legitimacy and its institutions (Freedom House, 2022; GEC, 2022).

Although less overtly disruptive than Russia – and less covered in the literature in comparison – China has pursued influence in the WB primarily through digital infrastructure, economic partnerships, and state-controlled media. Its Digital Silk Road projects, including the export of surveillance systems and innovative technologies, have created new forms of dependency that intersect with the region's information environment by shaping who controls data flows and communication infrastructures. At the narrative level, Chinese messaging promotes mutual respect and pragmatic economic cooperation, often presenting Beijing as a more reliable and responsive partner than Brussels, especially during the COVID-19 pandemic (GEC, 2022; CIDOB, 2023). While less aggressive than Russian information operations, these narratives nonetheless contribute to disinformation dynamics by selectively amplifying China's role and obscuring concerns over transparency, data protection, and accountability, thereby complicating EU efforts to define regional information integrity standards.

Turkey, meanwhile, leverages historical-cultural ties and Islamic solidarity, especially in Kosovo, Albania, and BiH, where its religious and media institutions promote conservative values and challenge Western liberal norms (CIDOB, 2023). These foreign influences intersect with domestic weaknesses in media regulation and political accountability. Across the region, state control or influence over public broadcasters, the proliferation of opaque online portals, and the absence of effective regulatory frameworks have left national information ecosystems vulnerable (Freedom House, 2022). In some cases, political elites act as disinformation agents themselves, deploying conspiratorial or nationalist narratives to discredit opponents and external actors, thereby reinforcing polarisation and impeding reform (Pamment et al., 2022, p. 7; CIDOB, 2023). These intertwined domestic and external disinformation practices highlight why the WB information environment is best seen as a site of strategic contestation rather than mere regulatory failure. Against this backdrop, the EU has attempted to position itself as a stabilising actor, advancing counter-disinformation and resilience measures in line with its broader digital sovereignty agenda.

Recognising the strategic threat posed by disinformation, the EU has sought to bolster resilience through both internal and external mechanisms and through at least two of the principles outlined in the previous part of

the study. The *Direct* logic and the EU's StratCom Task Force for the WB have played a central role in identifying hostile narratives, tracking malign actors, and supporting civil society in counter-disinformation efforts (European Commission, 2019). The EU has also been engaged in the region in the *Delegate* principle as it funded media literacy programs, journalist training, and data verification platforms across the region. However, their impact remains constrained by structural factors and the declining credibility of EU enlargement (Pamment et al., 2022, pp. 8–10).

The erosion of EU credibility is not merely a perceptual issue but reflects deeper institutional and political constraints. Juncker's 2014 declaration that there would be no enlargement during his mandate signalled a new context of enlargement fatigue, propelling both the stabilitocracy paradigm (Bieber, 2018) and set-back vis-à-vis the EU aims and goals in the region (Vladeva, 2014, p. 22). While the 2018 Strategy for the WB attempted to revive the enlargement agenda by framing it as a "strategic investment in a stable and united Europe" (European Commission, 2018), scholars argue that the EU's conditionality framework has lost much of its transformative capacity (Elbasani, 2013, p. 42; O'Brennan, 2014, p. 223). The tension between regional and bilateral approaches, coupled with enlargement fatigue among EU citizens – 49% of whom opposed further enlargement in 2013¹ (European Commission, 2013) – has further weakened the normative appeal of the EU model (Center for Southeast European Studies, 2014, p. 12).

Given the volatile geopolitical context and the intensifying global technological competition, this report examines how diverse digital sovereignty challenges unfold in the Western Balkans (WB), a region situated at the intersection of EU accession aspirations, security dependencies, and multipolar digital entanglements. A particular focus is placed on the role of disinformation as both a symptom and a strategic tool within these dynamics. Following an overview of the structural conditions shaping digital development in the region, this section is structured into several parts. It begins by introducing the specific features of digital dependency in the WB, tracing the historical and political roots of the current technological landscape.

The analysis then turns to the ways in which foreign actors, particularly the European Union, the United States, and China, exert influence through digital infrastructures, regulatory frameworks, and strategic partnerships. Crucially, it explores how this influence intersects with disinformation practices, including the projection of narratives, manipulation of information ecosystems, and co-optation of digital platforms. The report also considers how internal vulnerabilities, such as governance weaknesses, technological underdevelopment, and informal digital actors like hackers and disinformation brokers, further complicate sovereignty-building efforts. In its final part, the report reflects on these dynamics through the conceptual lenses of ontological security and assemblage theory, offering a more nuanced understanding of how regional actors navigate overlapping dependencies, strategic narratives, and incomplete forms of digital sovereignty.

Digital Strategies and Information Governance on the national level

While digitalisation is framed as a vehicle for modernisation and growth, most WB states have also begun acknowledging the growing threat of disinformation within their digital ecosystems. National strategies addressing disinformation remain fragmented, with some countries embedding counter-disinformation goals into broader cybersecurity or media policies, while others lack a dedicated approach. In practice, these strategies reflect uneven uptake of the logics outlined in the previous section. Albania and North Macedonia, for instance, have emphasised Delegate approaches by partnering with the EU and international

¹ In 2023, this percentage decreased to 37% (ECFR, 2023).

organisations to enhance media literacy, support fact-checking initiatives, and strengthen legal frameworks for online content moderation. Based on its cooperation with Estonia and Western donors, Kosovo has combined elements of Direct governance - by embedding information integrity into state-led e-governance reforms - with Delegate reliance on civil society. By contrast, Serbia and BiH have demonstrated minimal engagement with either logic: institutional coordination is weak, and political elites themselves sometimes act as disinformation agents, thereby undermining the Defend function of state institutions. Across the region, national efforts are often reactive and under-resourced, relying heavily on civil society and donor-driven projects rather than sustained state-led policies. In this respect, despite their interdependence, digital development and disinformation resilience are treated as separate policy tracks. This disjuncture limits the effectiveness of both efforts, as regulatory fragmentation, political capture, and infrastructural dependencies enable malign actors to exploit digital spaces with relative ease. The absence of a coherent application of *Defend*, *Direct*, and *Delegate* principles at the state level thus contributes to the region's ongoing vulnerability to both domestic and foreign disinformation campaigns.

Albania's Digital Agenda 2022–2026 stands out for its comprehensive framing of digital transformation. It outlines a multifaceted approach that ranges from improving e-governance and increasing public access to digital services to advancing cybersecurity protocols and facilitating Albania's international digital integration (The National Agency for Information Society, n.d.). The agenda positions technology not only as a means of improving administrative efficiency but also as a tool for fostering economic competitiveness and greater trust in public institutions. The Albanian government has emphasised that digitalisation is central to its development vision and frequently highlights its digital reforms in public diplomacy and international cooperation efforts. Albania has also taken steps to address disinformation through legislative reforms targeting online media transparency and content accountability, although critics warn these efforts risk restricting press freedom. The government has supported media literacy campaigns and partnered with the EU to monitor foreign information manipulation, particularly in the context of elections and regional security (BIRN, 2023).

By contrast, Bosnia and Herzegovina (BiH) faces significant institutional fragmentation, which complicates the implementation of a unified digital strategy. Despite this, several initiatives at the entity level aim to promote digital governance, economic modernisation, and digital infrastructure development. Notably, some strategies emphasise the role of digital transformation in bridging ethnic and administrative divides by fostering interoperability, transparency, and more coordinated policymaking processes (SSRC 2024). These efforts are often framed in technocratic and normative terms, especially when backed by foreign donors or international organisations. However, the country's fragmented governance structure complicates coherent responses to disinformation. Political elites in different entities often deploy conflicting narratives, and media regulation varies by jurisdiction, making coordinated action against foreign influence or domestic misinformation particularly difficult. Russian narratives find fertile ground in Republika Srpska, where political discourse often mirrors Kremlin-aligned messaging that undermines the legitimacy of BiH institutions (GEC 2020).

Kosovo has positioned itself as a digital reform leader in the region. Its Digital Agenda 2030 and e-Government Strategy 2023–2027 combine policy ambition with liberal-democratic values, explicitly seeking to avoid vendor lock-in, enhance civic participation, and ensure that technological development is compatible with human rights and public accountability principles. Notably, Kosovo has benefited from significant international support in implementing these goals, including from Estonia, a country widely regarded as a

global pioneer in e-governance (EGA, 2024). This partnership has provided logistical assistance and discursive legitimacy, reinforcing Kosovo's desire to align with best practices and digital governance norms in Northern Europe. In parallel, Kosovo has developed institutional frameworks for countering disinformation as part of its broader information security agenda. Given its contested international status, maintaining narrative legitimacy and public trust is considered a strategic imperative. This has prompted investments in fact-checking platforms, public awareness campaigns, and legal reforms aimed at combating foreign interference in digital media (EEAS 2024).

Montenegro's strategy has been heavily shaped by the experience of the COVID-19 pandemic, which emphasised the need for inclusive, flexible, and user-centric digital services. The country's digital transformation plan emphasises empathy and accessibility, underscoring the importance of designing systems that reflect the needs and preferences of users across different socio-economic and demographic groups (Cavanaugh, 2025). Montenegro has also worked to frame its digital modernisation to overcome administrative inefficiencies and strengthen its reputation as a regional innovator. Nevertheless, Montenegro has also struggled with politically motivated disinformation, particularly around electoral processes and anti-government protests. While formal counter-disinformation policies are minimal, the state has increasingly relied on ad hoc measures and cooperation with civil society groups to debunk falsehoods and mitigate online manipulation, especially during times of political crisis (Freedom House, 2022).

North Macedonia has adopted two complementary strategies that underscore its desire to integrate digital technologies across all sectors of society and the economy. Its National ICT Strategy 2021–2025 and Smart Specialisation Strategy 2024–2027 prioritise the development of digital infrastructure, e-services, and data analytics in support of economic sustainability and environmental protection (ITU, 2023). Significantly, North Macedonia's strategies draw heavily on EU models and aim to align national digital development with broader European integration goals. North Macedonia has also been a frequent target of Russian-backed disinformation, particularly around the Prespa Agreement and NATO accession. In response, it has partnered with the EU and NATO to develop early warning systems and strengthen strategic communication capacities within key state institutions. Nevertheless, the proliferation of online portals and foreign-backed media outlets continues to challenge information integrity (Doncheva & Svetoka, 2021).

Serbia, meanwhile, has arguably taken the most assertive approach to positioning itself as a digital leader in the region. The country has adopted several strategic frameworks aimed at promoting innovation, advancing public-private partnerships, and enhancing technological capacity. Of particular note is Serbia's AI Strategy 2025–2030, the first of its kind in the WB, which aims to establish the country as a regional centre for artificial intelligence research, development, and application (National AI Platform, 2025). This strategy is part of a broader attempt by Serbia to move up the global digital value chain and attract foreign investment in high-tech industries. Serbia's approach to disinformation is notably ambivalent. While the government participates in some EU and US-led digital capacity-building programs, it also tolerates, and at times enables, pro-Russian and anti-Western narratives through aligned media outlets. This dual-track approach allows Serbia to maintain strategic ambiguity in its geopolitical orientation, while using disinformation domestically to consolidate power and discredit opposition voices (Doncheva & Svetoka, 2021).

Despite their ambitious tone, these strategies are often better understood as expressions of aspiration rather than reflections of current capacity. They serve as performative markers of modernity, signalling alignment with EU priorities and global best practices, even when domestic implementation remains constrained. Across

the region, political elites are increasingly aware that sustaining political legitimacy in the digital age requires some degree of control over technological infrastructure, platform governance, and data flows. The rise of cybercrime, disinformation, and technological dependence has reinforced this perception (BIRN 2023; GIATOC 2024).

However, the tools available to achieve genuine digital sovereignty remain limited. At the same time, many WB governments are trying to leverage technology as an economic development tool. Countries seek to position themselves as attractive locations for IT outsourcing, digital entrepreneurship, and even digital nomadism. These narratives are often couched in language that blends economic modernisation with cosmopolitanism, arguing that digital integration is key to attracting investment and reversing brain drain (Djurickovic, 2025). However, these aspirations exist alongside deep structural limitations, ranging from underfunded institutions and political instability to lack of skilled labour and infrastructural deficits, often undermining meaningful progress. These country-level strategies, however ambitious, operate within a structural environment of dependency. The region's digital ecosystems remain shaped less by endogenous capacity than by external infrastructures, platforms, and regulatory models. It is within this broader condition of dependency that foreign actors, above all the U.S., China, and the EU, exert influence and compete for normative authority.

Sovereignty deficiencies amid emerging digital multipolarity

The WB journey toward digital sovereignty has not occurred in a vacuum. It has evolved in a global environment marked by shifting geopolitical alignments, emerging technological powers, and increasing tensions over the control of digital infrastructures, standards, and values. The region's experience can be divided into several key phases, each reflecting broader transformations in the international system and the role of technology in statecraft. In the 2000s, the EU exercised considerable normative influence in the WB, positioning itself as both a model and patron of digital modernisation. During this period, digital development was largely seen as a technical component of the broader reform agenda tied to European integration. Regulatory harmonisation with the EU *acquis* was prioritised over digital autonomy. Technology was framed primarily in administrative and economic terms, and digital capacity was mostly developed through foreign aid and technical assistance.

The global financial crisis of 2008–2009 marked a turning point. As the EU's economic and political capacity weakened, space opened for alternative actors to offer development models and technological partnerships. China emerged as a key player during this time, expanding its presence through both economic investment and digital infrastructure projects. The arrival of Chinese firms, such as Huawei and ZTE, challenged the EU's monopolistic influence and introduced new strategic choices for WB governments. By the late 2010s, the United States had become increasingly concerned with China's expanding technological footprint. In response, it launched the Clean Network Initiative (CNI), an effort to build a global coalition committed to excluding Chinese companies from critical digital infrastructure projects. This initiative was presented as a values-based project to protect data integrity, democratic norms, and national sovereignty. In parallel, the EU revitalised its Digital Agenda for the Western Balkans (2018 onward), reframing digital policy in geopolitical terms.

While comparisons to Global South digital trajectories are useful in understanding structural dependencies and asymmetries, the WB context includes unique institutional and political features. These include the EU

accession framework, NATO alignment, and historically embedded security dependencies. WB states face compounded challenges: small market size, limited institutional maturity, and a semi-peripheral status in both economic and technological terms. Their sovereignty deficits – weak infrastructure control, porous regulatory systems, and politicised technology procurement – are deeply structural and not easily overcome. Historically, the region has functioned as a geopolitical interface between great powers. Today, this role continues, albeit in new digital forms. The WB remains embedded in asymmetric relationships with actors such as the US, China, Russia, Turkey, the post-Brexit UK, and individual EU member states. While this external competition provides local elites with room to manoeuvre and extract concessions, it also exposes the region to overlapping and often contradictory agendas, particularly in the digital domain.

This pluralisation of influence might appear as a form of healthy diversification. However, in a context marked by low trust, weak institutions, and fragmented regulatory regimes, diversification often results in fragmentation and strategic vulnerability. Digital infrastructures have become central to national security calculations, and the choice of technological partners increasingly resembles military procurement decisions – where vendors are also potential surveillance nodes, intelligence actors, or coercive instruments. Rising cybersecurity threats further illustrate the region's precarious situation. The Balkans have witnessed an increase in cyberattacks targeting both state institutions and private entities (BIRN, 2023; GIATOC, 2024). As digital networks grow in scale and complexity, so too does their susceptibility to penetration, manipulation, and systemic disruption. These vulnerabilities are exacerbated by the region's reliance on external platforms and infrastructure.

Digital sovereignty in the WB, therefore, is not simply about technological autonomy. It is about strategic navigation within fragmented, overlapping digital ecosystems that often lack interoperability and impose incompatible regulatory expectations. Local decision-making is constrained by both economic incentives and security dilemmas. Countries are not choosing technologies in a neutral marketplace; they are aligning themselves with power blocs, each offering different political, normative, and infrastructural models.

Digital dependency, tech integration and FIMI

The digital environment in the WB remains structurally dependent on Western technological systems. Since the fall of state socialism, the region has looked to the West not only for hardware and software but also for regulatory models and conceptual frameworks. American firms are dominant in the digital services sphere. Microsoft, Google, Amazon Web Services, Meta, Cisco, and Oracle provide everything from office software and cloud computing to social media and messaging platforms. These platforms have become infrastructural, often playing quasi-sovereign roles in data governance, content moderation, and public communication. In recent years, digital technologies have evolved from tools of administrative efficiency into central instruments of state capacity, strategic foresight, and security governance. This shift is exemplified by the so-called “Palantir moment” (Vlassis, 2024), where states increasingly outsource not only data storage and analysis but also key policy decisions and predictive functions to private, often opaque, technology firms.

Such delegation can compromise democratic oversight, particularly when algorithmic decision-making becomes embedded in core state functions. China's rise has further complicated this dynamic by offering a model of digital-state integration known as “techno-statism” (Zhang, 2024), in which surveillance, artificial intelligence, and big data are fused into a cohesive system of state control. As these systems are exported to semi-peripheral regions like the WB, they reshape not only infrastructure but also the contours of the public sphere. Disinformation thrives in environments where infrastructures are opaque, content governance is

externally controlled, and accountability mechanisms are weak or absent. Both Western and Chinese systems, in different ways, risk crowding out pluralistic debate and eroding the epistemic foundations of liberal democracy. As control over digital infrastructures becomes decoupled from democratic norms, the capacity to identify, resist, and counter disinformation is undermined, allowing narrative manipulation, social polarisation, and political distrust to take deeper root in already fragile democracies.

These dynamics underline that digital dependency in the WB is not only a technical or economic matter but also a deeply political one. As Western platforms and Chinese techno-statist systems structure the region's digital ecosystems, they simultaneously shape the conditions under which disinformation circulates and public authority is contested. The question, therefore, is how regional actors, and above all the EU, respond to this environment of overlapping dependencies. The EU's efforts to project digital sovereignty can be read as an attempt to reassert regulatory control, embed liberal-democratic norms into technological infrastructures, and position itself as the region's primary normative anchor.

EU's digital sovereignty projection

The European Union has long sought to project its regulatory power as a form of soft sovereignty. Within the EU itself, digital sovereignty is now seen as essential for protecting both security and European values. The concept encompasses territorial control over digital infrastructure, economic competitiveness in emerging tech sectors, and normative leadership in areas like data protection and content regulation, including reaction to disinformation and FIMI (Adler-Niessen & Eggerling, 2024). Traditionally, the EU has led globally in digital governance through its market power and regulatory innovation, most notably with GDPR. However, in recent years, security concerns have taken precedence. Efforts are underway to expand digital sovereignty beyond economic governance to areas such as digital finance (Donnelly et al., 2024), (Flonk et al., 2024), and cybersecurity.

The notion of defending a "European way of life" through technological control points to the increasingly ideological dimension of EU digital strategy. This means that digital governance is no longer seen solely as a matter of market regulation or consumer protection, but as a vehicle for safeguarding core European values such as privacy, human rights, rule of law, and democratic accountability; all within the architecture of digital systems. It reflects a normative stance that technological design, platform governance, and data management must embody liberal-democratic principles, especially in contrast to authoritarian models that prioritise surveillance and state control (Lambach & Oppermann, 2022). In the context of the WB, this ideological framing reinforces the EU's attempt to position itself as a normative power, though it may also heighten tensions with local actors who view such conditionality as intrusive or politically selective.

In the WB, the EU remains the most committed external actor in terms of capacity-building, funding, and institutional support. Its Digital Agenda for the Western Balkans (launched in 2018) aimed to foster broadband connectivity, e-governance, cybersecurity, and digital inclusion (European Commission, 2018b). Yet, despite the scale of its investments, the EU's impact is often perceived as smaller and more conditional than that of other actors, particularly China and the US.

A similar asymmetry characterises the EU's counter-disinformation strategy in the WB. While the EU has invested in media literacy programs, fact-checking networks, and civil society partnerships, often through the European External Action Service's StratCom Task Force (2024), these efforts are primarily top-down and externally driven. WB governments are frequently treated as implementation partners rather than equal stakeholders in designing strategic communication frameworks. The EU sets the normative agenda around

“resilience” and “information integrity,” but leaves limited space for local input on how these concepts align with domestic political realities. Moreover, the emphasis on countering foreign disinformation, particularly from Russia, often overlooks the internal disinformation ecosystems shaped by clientelism, party media, and elite manipulation. As with digital regulation more broadly, the region adopts counter-disinformation norms in a compliance-oriented fashion, without the institutional autonomy or political capital to localise them meaningfully. This reinforces a broader pattern in which the EU’s digital and information governance tools risk reproducing dependency rather than fostering genuine sovereignty.

Despite this, the EU continues to invest in capacity-building programs, training schemes, and public-private partnerships that promote regulatory alignment and institutional reform (RCC, n.d.; WBIF, n.d.). These initiatives provide valuable technical assistance but often lack the visibility and political capital of Chinese infrastructure or American platforms. The EU’s credibility is further undermined by enlargement fatigue, inconsistent conditionality, and its failure to counterbalance the commercial dominance of non-European tech companies (Varoufakis, 2024; Rolf & Schindler, 2023). Local elites increasingly regard EU norms as “checkbox requirements” rather than transformative frameworks. Reform is pursued selectively, often framed in instrumental terms to unlock funding or satisfy minimal compliance.

Digital Silk Road? China’s role in the Western Balkans

In response to the 2008–2009 Global Financial Crisis, China launched the Belt and Road Initiative (BRI), a wide-reaching policy framework that consolidates various domestic and foreign policy objectives under a single geoeconomic vision. The initiative promotes connectivity across domains such as economic policy coordination, trade and investment flows, and especially the development of transport and energy infrastructure, which has become its most recognisable component (Beeson, 2018; Vangeli, 2018; Ye, 2020). Aligned with the BRI is the Digital Silk Road (DSR), a banner term describing China’s international efforts to globalise its technology sector, promote digital infrastructure and digitisation, foster e-commerce and digital economy growth, and create new dialogues around standards and regulation.

The DSR, like BRI, is not a centralised or top-down initiative. It is shaped by a mix of Chinese state and non-state actors, including digital companies, local governments, and other stakeholders (Cheng & Zeng, 2024). DSR participation is voluntary and selective, often structured around expos and showcases where countries can learn about China’s technological offerings and choose the elements that align with their development needs. The domestic function of DSR, much like BRI, is to support the global expansion of Chinese digital companies. While the political framework is set by central institutions, the practical implementation is delegated to companies and local actors. In the West, however, DSR is commonly portrayed as a coordinated and strategic project intended to export China’s model of digital governance. Critics argue it promotes digital authoritarianism or even totalitarianism through tools like surveillance systems and state-controlled platforms (Qiang, 2019; Cheney, 2019; Bradford, 2023).

Placing DSR in a broader historical context shows continuity with China’s long-term strategy of embedding itself in global and regional technological systems. Since the early 2000s, China has signed Economic and Technology Cooperation (EATC) agreements with WB states. AidData research (Custer et al., 2023) and recent analyses (McFaul & Engelke, 2025) suggest that many of China’s digital projects in the Balkans may go unrecorded or unrecognised because they are embedded in sectors like education, agriculture, or healthcare, which now increasingly feature digital elements. Major Chinese tech firms such as Huawei, ZTE,

and Alibaba operate in the region, often independently, supporting e-government, broadband rollout, and training programs.

American response: Clean Network Initiative

In the U.S. mission to directly respond to China's Digital Silk Road (DSR), enlisting global and regional partners became a central strategic goal. One of the most visible expressions of this was the launch of the Clean Network Initiative (CNI), which aimed to build an alliance of countries committed to protecting data rights and democratic principles within digital systems. The initiative positioned itself as a safeguard against unnamed authoritarian actors extending their digital influence (U.S. Embassy & Consulates in the United Kingdom, n.d.). Becoming a CNI signatory came with a clear political commitment: countries were expected to ban untrusted vendors, particularly Chinese companies, from supplying critical 5G infrastructure (America's Cyber Defence Agency, n.d.-b). While the United States had previously supported other digital governance initiatives in the WB, including capacity-building through USAID and cybersecurity training programs, the CNI marked a more forceful effort to shape the region's digital trajectory.

Unlike these softer measures, the CNI was advanced through high-level diplomatic pressure. Then-Secretary of State Mike Pompeo's 2019 visit to the Balkans (Brunnstrom, 2019), part of a broader campaign across Central and Eastern Europe, served as a direct warning against expanding Chinese digital infrastructure. This was accompanied by public calls to exclude Huawei and ZTE based on security risks (Limitone, 2019). By that point, Huawei had already positioned itself as a preferred partner for many countries due to its affordability and technological readiness (Umbach, 2020). This situation gave rise to a dilemma: either advance digital development with Huawei's support or prioritise national security by excluding it. Kaska et al. (2019) describe this as a form of security dilemma, in which national interest is split between short-term development goals and long-term strategic risk.

Within the European Union, several countries aligned with the U.S. view and moved to restrict Huawei's role in their 5G infrastructure. However, not all EU member states agreed that exclusion was necessary or effective (Cheng & Zeng, 2024). In contrast, WB governments were quicker to side with Washington. After Pompeo's outreach, Albania, Kosovo, and North Macedonia signed on to the CNI (Salihu, 2023). Serbia also made a formal commitment by signing the Washington Agreement at the White House. President Vučić's appearance beside President Trump signalled intent to block Chinese vendors from the country's 5G market (Ruge & Vladislavljev, 2021), though this did not lead to a meaningful change in Serbia's relations with Huawei. In contrast, Albania, Kosovo, and North Macedonia took firmer steps to exclude Chinese vendors. Albania was the first to align with the U.S. position (Vladiavljev, 2021), while North Macedonia reversed earlier cooperation with Huawei and ZTE despite past strategic partnerships (Government of the Republic of North Macedonia, 2015; 2017).

Overall, the U.S. campaign has seen partial success. While some states excluded Chinese tech, others remain closely engaged. The U.S. increasingly views the Balkans as part of its broader cyberdefense perimeter, not only through NATO (NATO, 2023) but via bilateral arrangements (Bodine & Kennedy, 2025). In this view, the U.S. is not only a development partner but a guarantor of regional digital sovereignty, anchoring cybersecurity within formal security alliances rather than informal networks (Farrell & Newman, 2023). Since the initial push around the CNI, U.S. engagement in the WB's digital space has shifted from

vendor exclusion toward broader frameworks of cyber governance, institutional resilience, and regional interoperability. As geopolitical competition in the digital realm intensifies, the Western Balkans is likely to remain a testing ground for hybrid models of governance, where U.S., EU, and Chinese influences intersect and compete in increasingly subtle and strategic ways.

Conceptual Reflections: Ontological Security and Assemblage Perspective as determinants of the Western Balkans' digital policies

To understand how states in the WB navigate fragmented digital dependencies, FIMI challenges and how they relate to the European FIMI efforts in the neighbourhood requires conceptual tools that capture both identity-driven anxieties and the fluidity of geopolitical and technological arrangements. Ontological security theory (OST) and the assemblage perspective, though distinct in origins and scope, provide such tools. Together, they allow us to explore how states seek to stabilise their sense of self while managing the often contradictory elements of external influence and internal fragility.

Kosovo's adoption of advanced e-governance frameworks, supported by partners like Estonia, serves not only practical goals but also symbolic ones: projecting the image of a modern, technologically competent, and values-aligned democracy (EGA, 2024). Similarly, Serbia's balancing between US, EU, and Chinese technological partnerships reflects a broader identity narrative grounded in strategic autonomy and regional leadership. As Rumelili (2015) notes, actors may seek ontological security not only through stable relationships but also through resistance to perceived domination or imposition. This helps explain Serbia's embrace of Huawei while formally aligning with some US and EU digital initiatives. The coherence of identity can sometimes take precedence over coherence in policy. However, the pursuit of ontological security in fractured political contexts often leads to paradoxes. States may become attached to routines or alliances that no longer serve their material interests. Croft (2012) and Browning and Joenniemi (2017) argue that this attachment to identity continuity can reinforce insecurity when it prevents adaptation or reform. In BiH, for example, fragmented digital governance persists not simply because of institutional weakness, but also because it reflects the underlying ethno-political structure that many actors are invested in maintaining for narrative reasons.

Disinformation, in this context, can function as both a symptom and a tool of ontological security-seeking. States or political elites may tolerate or even cultivate disinformation ecosystems when they serve to reinforce identity narratives or deflect pressures for reform. In Serbia, for instance, disinformation aligned with pro-Russian or anti-Western discourses helps sustain the narrative of strategic autonomy and national exceptionalism. This allows political actors to reconcile contradictory alignments, such as partnerships with both Huawei and the EU, by appealing to a deeper coherence grounded in national identity rather than policy consistency. In BiH, disinformation further entrenches the ethno-political divisions that underlie the state's fragmented governance. Competing narratives about state legitimacy, sovereignty, and foreign influence circulate through partisan media ecosystems, often supported or tolerated by political elites. These narratives not only reproduce ontological attachments to group identity but also hinder the emergence of a shared public sphere necessary for institutional reform or digital coordination. As such, disinformation is not just a threat to liberal norms or external stability; it is a constitutive part of the assemblage through which fractured states like BiH sustain internal political order and resist transformative change.

In this context, digital governance and attempts to counter FIMI are best seen as a complex assemblage of widely different actors. It involves local ministries, international donors (including the EU), multinational corporations, civil society organisations, and global platforms. These are not coordinated through a single sovereign framework but coexist in a fluid and often contradictory way. While different regional states might have their own policies aimed at countering FIMI and broader digital governance, these coexist with the assemblages of the EU's practices pursued following the delegate organising principle and support for the local civil society.

Assemblage theory also challenges clear-cut notions of foreign influence. This reflects what Collier and Ong (2005) call global assemblages: standardised forms such as GDPR that are adopted and adapted in local contexts according to contingent logics. While China or the US may offer packages of technology and governance norms, their implementation in the region is subject to translation, resistance, and hybridisation. As Chacko and Jayasuriya (2017) argue, assemblages do not obey top-down logics. Instead, they are shaped through negotiation and partial connections. Thus, Serbia's Huawei surveillance projects may carry over Chinese technological templates but operate through local discourses of public safety, modernity, and sovereignty. The intersection of OST and assemblage thinking reveals that digital sovereignty in the WB is neither a stable goal nor a linear process. It is a negotiated and relational phenomenon. The pursuit of ontological security motivates actors to engage with multiple digital systems and pursue different countering FIMI policies that reaffirm their identity narratives. At the same time, the actual configuration of digital governance is fragmented, contingent, and multi-scalar.

Summary: Digital politics between identity-seeking and fragmented assemblages

These insights carry important implications for policymakers. First, efforts to support digital sovereignty in the WB must acknowledge that technical alignment and capacity-building are inseparable from identity politics and legitimacy narratives. Policies that assume linear progress toward EU norms or full regulatory harmonisation risk overlooking the political uses of fragmentation and the performative dimensions of digital alignment. Second, interventions should be designed with the understanding that governance in the region emerges from dynamic assemblages, composed of state and non-state actors, digital infrastructures, and competing narratives, which require adaptive, context-specific engagement. This means privileging flexible, multi-scalar cooperation over rigid conditionality, and fostering local agency in shaping digital futures. Finally, counter-disinformation strategies should be embedded within this broader understanding of digital order, moving beyond reactive fact-checking to address the structural and narrative conditions that make disinformation both functional and attractive to political elites. Without addressing these deeper dynamics, digital interventions are likely to reproduce the very dependencies and insecurities they aim to resolve.

Conclusions and policy recommendations

In this report, we unpack the EU's approach to countering disinformation and FIMI inside the EU and contrast it with a fragmented landscape of digital governance in the Western Balkans, which is one of the areas where the EU exports its digital policies. On the EU level, we identify three main organising principles connected to the ontological security of the EU as a liberal actor in different domains and giving rise to variously composed assemblages. In the Western Balkans, we point out the diverging and fragmented digital policies that exist in the context of the great power rivalry and multiple political projects informed by ontological security seeking. This translates to alignment in different assemblages informed by widely different logics.

In the conclusion, we translate our observations into specific policy recommendations both for the EU as such and for its engagement in the Western Balkans.

On the EU level,

1. The EU must more clearly define its strategy towards achieving digital sovereignty. This ambition has to be aligned and based on its fundamental principles of freedom, the rule of law and equality. Only by defining this vision will the EU be able to build a mode of governance that will be a viable alternative to those promoted by the United States, China or Russia. We believe that due to its ability to address ontological insecurity without compromising individual freedom or democratic principles, the EU's vision of digital sovereignty can have global appeal and serve to enhance its soft power. We consider the principles outlined in the Action Plan on Disinformation in 2018 a reasonable and realistic basis for politics related to this issue. At the same time, we encourage the European Commission to propose more specific, measurable, and goal-oriented strategies in its 3D framework.
2. The European Commission, in close cooperation with member states and civil society, should continue to uncover FIMI, aiming to undermine security and social cohesion in the EU. These attempts should be countered with legal and diplomatic means that should deter potential malign actors. At the same time, the EU should make a clear distinction between illegitimate FIMI and transparent public diplomacy that might serve as an important venue for exchanging ideas, forging people-to-people contacts and de-escalating conflicts.
3. The Digital Service Act is an important step in the ambition to regulate the information space. However, social platforms' compliance with this legislation has to be properly overseen in cooperation with researchers and civil society. At the same time, the European Commission has to remain open to conversation with platforms in order to search for technically achievable, viable, and transparent solutions. The main aim has to be the protection of the rights of European citizens as individuals as well as consumers.

In the Western Balkans,

1. The EU should support the integration of disinformation and digital development strategies. As shown in our analysis of WB national digital agendas, governments frequently pursue digital modernisation and disinformation resilience as separate policy tracks, with the latter often underfunded or outsourced to donors (Freedom House, 2022; BIRN, 2023). This institutional separation creates vulnerabilities, since infrastructural dependencies and opaque platform governance directly shape the conditions under which disinformation circulates. Regional governments, with EU support, should therefore embed information integrity and counter-disinformation objectives into their broader digital

transformation strategies, rather than treating them as reactive add-ons. This would align resilience-building with infrastructural reforms and ensure that investments in connectivity, e-governance, and cybersecurity are also leveraged to strengthen the information environment.

2. The EU should make sure that the regional states pursue counter-FIMI and counter-disinformation and move beyond compliance-driven EU alignment. Our analysis demonstrates that EU counter-disinformation initiatives in the WB are largely externally driven, with governments positioned as implementation partners rather than equal stakeholders (Pamment et al., 2022). This compliance-oriented dynamic risks reinforcing perceptions of dependency and undermining the EU's normative credibility. Instead, the EU should adopt a more participatory approach by co-designing resilience frameworks with local actors, including independent media, fact-checking organisations, and civic groups and thus align more strongly with the *Delegate* principle. This would not only increase local ownership but also help adapt EU frameworks to the political and media realities of WB states, where disinformation is often endogenous and elite-driven, rather than purely externally orchestrated.
3. The EU and its local partners need to target structural vulnerabilities alongside narrative interventions. Disinformation in the WB is not merely a matter of false narratives; it thrives in institutional contexts marked by political capture of media, fragmented regulatory frameworks, and weak public trust (GEC, 2022; Freedom House, 2022). EU and U.S. initiatives often prioritise fact-checking and media literacy, but our analysis shows that without addressing these structural enablers, such measures have limited impact. Counter-disinformation strategies must therefore be broadened to include reforms of media regulation, safeguards against political interference in public broadcasters, and capacity-building for independent oversight bodies. Only by addressing both structural and narrative drivers can the information environment be made more resilient.
4. The EU should foster adaptive, multi-scalar cooperation with its regional partners, following the *Direct* and *Delegate* principles. As the assemblage perspective highlights, digital governance in the WB emerges from hybrid configurations involving governments, international donors, global tech firms, and local civic actors. Rigid conditionality or binary vendor exclusion policies, such as those promoted under the Clean Network Initiative, risk reinforcing fragmentation or alienating local stakeholders. Instead, external actors should privilege flexible, multi-scalar forms of cooperation that can adapt to local contexts while promoting interoperability with Euro-Atlantic standards. This could include supporting regional cyber hubs, encouraging public–private partnerships that include civil society, and aligning donor programs to avoid duplication and overload.
5. The EU should address ontological security concerns directly. Our conceptual framework shows that disinformation often serves as a tool of ontological security-seeking, reinforcing identity narratives and legitimising elite strategies. Policies that ignore these identity dynamics risk technical success but political failure. Counter-disinformation and digital sovereignty initiatives should therefore be designed with narrative legitimacy in mind, engaging with how reforms are framed and understood domestically. For instance, supporting inclusive narratives around European integration and democratic modernisation can reduce the appeal of conspiratorial or divisive discourses. This requires careful communication strategies, tailored media campaigns, and partnerships with local opinion leaders who can translate technical norms into politically resonant terms.

References

- 1) Acuto, M., & Curtis, S. (2014). Reassembling international theory: Assemblage thinking and international relations. *Palgrave Macmillan*.
- 2) Adler, E., & Drieschova, A. (2021). The Epistemological Challenge of Truth Subversion to the Liberal International Order. *International Organization*, 75(2), 359–386. <https://doi.org/10.1017/S0020818320000533>.
- 3) Adler-Nissen, R., & Eggeling, K. A. (2024). The discursive struggle for digital sovereignty: Security, economy, rights and the Cloud project Gaia-X. *Journal of Common Market Studies*, 62(4), 993–1011. <https://doi.org/10.1111/jcms.13594>
- 4) Barbulescu, R., & Troncota, D. (2012). EU's enlargement policy towards Western Balkans: Between Europeanisation and reconciliation. *Romanian Journal of European Affairs*, 12(4), 103–120.
- 5) Barry, A. (2013). *Material Politics: Disputes Along the Pipeline*. Oxford University Press.
- 6) Beeson, M. (2018). Geoeconomics with Chinese characteristics: The BRI and China's evolving grand strategy. *Economic and Political Studies*, 6(3), 240–256. <https://doi.org/10.1080/20954816.2018.1498988>
- 7) Bieber, F. (2020). *The rise of authoritarianism in the Western Balkans*. Palgrave Macmillan.
- 8) BIRN. (2023). Battle for Balkan cybersecurity: Threats and implications of biometrics and digital identity. *Balkan Insight*. <https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/>
- 9) Blockmans, S. (2004). EU enlargement and the rule of law: The case of Montenegro. In *The EU and the Western Balkans* (pp. 310–327). T.M.C. Asser Press.
- 10) Bouza García, L., & Oleart, A. (2024). Regulating Disinformation and Big Tech in the EU: A Research Agenda on the Institutional Strategies, Public Spheres and Analytical Challenges. *JCMS: Journal of Common Market Studies*, 62(5), 1395–1407. <https://doi.org/10.1111/jcms.13548>.
- 11) Börzel, T. A. (2011). *When Europeanization hits limited statehood: The Western Balkans as a test case for the transformative power of Europe* (KFG Working Paper Series No. 30). Freie Universität Berlin.
- 12) Bradford, A. (2023). *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.
- 13) Browning, C. S., & Joenniemi, P. (2017). Ontological security, self-articulation and the securitization of identity. *Cooperation and Conflict*, 52(1), 31–47.
- 14) Brunnstrom, D. (2019). “Pompeo Warns about Chinese Influence in Balkans.” *Reuters*, <https://www.reuters.com/article/world/pompeo-warns-about-chinese-influence-in-balkans-idUSKBN1WJ0TZ/>.
- 15) Carver, J. (2024). More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. *Journal of European Public Policy*, 31(8), 2250–2286. <https://doi.org/10.1080/13501763.2023.2295523>
- 16) Casero-Ripollés, A., Tuñón, J. & Bouza-García, L. (2023). The European approach to online disinformation: geopolitical and regulatory dissonance. *Humanities and Social Sciences Communications*, 10, 657.

- 17) Cavanaugh, L. (2025). "How Empathy Became a Digital Government Superpower in Montenegro and the US." *GovInsider*. <https://govinsider.asia/intl-en/article/how-empathy-became-a-digital-government-superpower-in-montenegro-and-the-us>.
- 18) Chacko, P., & Jayasuriya, K. (2017). International order and the politics of transitional governance: From benchmarking to surveillance. *International Politics*, 54(1), 36–51.
- 19) Cheng, J., & Zeng, J. (2024). 'Digital Silk Road' as a slogan instead of a grand strategy. *Journal of Contemporary China*, 33(149), 823–838. <https://doi.org/10.1080/10670564.2023.2222269>
- 20) Conrad, M. (2025). *Reclaiming the Epistemic Basis of Liberal Democracy*. Reclaim. [https://ams.overcastcdn.com/documents/RECLAIM Discussion Paper 2025 1 Max pn.pdf](https://ams.overcastcdn.com/documents/RECLAIM_Discussion_Paper_2025_1_Max_pn.pdf).
- 21) Collier, S. J., & Ong, A. (2005). Global assemblages, anthropological problems. In A. Ong & S. J. Collier (Eds.), *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems* (pp. 3–21). Blackwell.
- 22) Croft, S. (2012). Constructing ontological insecurity: The securitization of Britain's Muslims. *Contemporary Security Policy*, 33(2), 219–235.
- 23) Custer, S. (2023). *Tracking Chinese Development Finance: An Application of AidData's TUFF 3.0 Methodology*. Williamsburg, VA: AidData at William & Mary.
- 24) Datzer, V., & Lonardo, L. (2023). Genesis and evolution of EU anti disinformation policy: Entrepreneurship and political opportunism in the regulation of digital technology. *Journal of European Integration*, 45(5), 751–766. <https://doi.org/10.1080/07036337.2022.2150842>.
- 25) Dityrch, O. (2024). *D6.1 –Concepts, Methods and Planning Document*, Reclaim.
- 26) Dityrch, O., Eberle, J., Monsees, L. & Kratochvíl, P. (2025). *Reimagining the International as a Challenge to Liberal Democracy*. Reclaim. [https://ams.overcastcdn.com/documents/RECLAIM Discussion Papers 2025 2 IIRP.pdf](https://ams.overcastcdn.com/documents/RECLAIM_Discussion_Papers_2025_2_IIRP.pdf).
- 27) de Goede, M., & Simon, S. (2013). Governing Future Radicals in Europe. *Antipode*, 45(2), 315–335. <https://doi.org/10.1111/j.1467-8330.2012.01039.x>.
- 28) Deleuze, G., & Guattari, F. (1987). *A Thousand Plateaus: Capitalism and Schizophrenia*. University of Minnesota Press.
- 29) Doncheva, T., & Svetoka, S. (2021, October 27). *Russia's footprint in the Western Balkan information environment: Susceptibility to Russian influence*. NATO Strategic Communications Centre of Excellence. <https://stratcomcoe.org/publications/russias-footprint-in-the-western-balkan-information-environment-susceptibility-to-russian-influence/216>
- 30) Donnelly, S., Ríos Camacho, E., & Heidebrecht, S. (2024). Digital sovereignty as control: The regulation of digital finance in the European Union. *Journal of European Public Policy*, 31(8), 2226–2249. <https://doi.org/10.1080/13501763.2023.2295520>
- 31) EGA (2024). e-Governance Academy Kosovo Report. *Estonian e-Governance Academy*. <https://ega.ee/kosovo-digital-agenda-2024>
- 32) Elbasani, A. (2013). *European Integration and Transformation in the Western Balkans: Europeanization or Business as Usual?* Routledge.
- 33) EUR-lex. (2022). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS On the European democracy action plan*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&gid=1607079662423>

- 34) EUR-lex. (2024). *Transparency and targeting of political advertising*. <https://eur-lex.europa.eu/EN/legal-content/summary/transparency-and-targeting-of-political-advertising.html>
- 35) European Commission. (n.d.-a.) *Strategic communication and countering foreign information manipulation and interference*. https://commission.europa.eu/topics/countering-information-manipulation_en
- 36) European Commission (n.d.-b). *Topics*. https://commission.europa.eu/topics_en
- 37) European Commission (n.d.-c). *AI Act*. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- 38) European Commission (n.d.-d). *Sanctions against individuals, companies and organisations*. https://commission.europa.eu/topics/eu-solidarity-ukraine/eu-sanctions-against-russia-following-invasion-ukraine/sanctions-against-individuals-companies-and-organisations_en
- 39) European Commission (n.d.-e). *DSA: Making the online world safer*. <https://digital-strategy.ec.europa.eu/en/policies/safer-online>
- 40) European Commission (n.d.-f). *The 2022 Code of Practice on Disinformation*. <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>
- 41) European Commission (n.d.-g). *Cooperating with fact-checkers, civil society, media and academia*. Accessed October 10, 2025. https://commission.europa.eu/topics/countering-information-manipulation/cooperating-fact-checkers-civil-society-media-and-academia_en
- 42) European Commission. (2011). *Enlargement Strategy and Main Challenges 2011–2012*. Brussels.
- 43) European Commission. (2013). *Standard Eurobarometer 79: Public Opinion in the EU*. Spring 2013.
- 44) European Commission. (2016). *Security: EU strengthens response to hybrid threats*. https://ec.europa.eu/commission/presscorner/detail/en/ip_16_1227
- 45) European Commission. (2018a). “Action Plan on disinformation: Commission contribution to the European Council (13-14 December 2018).” https://commission.europa.eu/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en
- 46) European Commission. (2018b). “European Commission Launches Digital Agenda for the Western Balkans.” https://ec.europa.eu/commission/presscorner/detail/es/ip_18_4242.
- 47) European Commission. (2024). *Report: Safer Together – Strengthening Europe’s Civilian and Military Preparedness and Readiness*. https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en
- 48) European External Action Service. (2022). *2021 Stratcom Activity Report*. <https://www.eeas.europa.eu/sites/default/files/documents/Report%20Stratcom%20activities%202021.pdf>
- 49) European External Action Service. (2024). *Global media communities gather in Pristina, Kosovo to fight disinformation*. https://www.eeas.europa.eu/eeas/global-media-communities-gather-pristina-kosovo-fight-disinformation_en
- 50) European External Action Service. (2025a). *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)*. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
- 51) European External Action Service. (2025b). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

- 52) EUvsDisinfo (2023a). 'To Challenge Russia's Ongoing Disinformation Campaigns': Eight Years of EUvsDisinfo. <https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-eight-years-of-euvsdisinfo/>
- 53) EUvsDisinfo. (2023b). "Weaponising weapons deliveries." <https://euvsdisinfo.eu/weaponising-weapons-deliveries/>
- 54) Falkner, G., Heidebrecht, S., Obendiek, A. & Seidl, T. (2024). Digital sovereignty - Rhetoric and reality. *Journal of European Public Policy*, 31(8), 2099–2120. <https://doi.org/10.1080/13501763.2024.2358984>
- 55) Farrell, H., & Newman, A. (2023). *Underground empire: How America weaponized the world economy*. Henry Holt and Company..
- 56) Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the EU: towards digital sovereignty. *Journal of European Public Policy*, 31(8), 2316–2342. <https://doi.org/10.1080/13501763.2024.2309179>
- 57) Freedom House. (2022). *Freedom in the world 2022: Montenegro*. <https://freedomhouse.org/country/montenegro/freedom-world/2022>
- 58) Freedom House. (2022). *Nations in Transit 2022: Dropping the Democratic Façade*. <https://freedomhouse.org/report/nations-transit/2020/dropping-democratic-facade>.
- 59) García-Gordillo, M., Rivas-de-Roca, R., & de-Lima-Santos, M.-F. (2025). The Fact-Checking Initiatives in the EU: A Diverse Ecosystem Against Disinformation. *Media and Communication*, 13(0). <https://doi.org/10.17645/mac.9421>
- 60) García-Gutián, E., Bouza, L., & Haapala, T. (2024). What Is the EU's Vision of Democracy in the Post-Truth Scenario? A Conceptual Analysis of the Institutional Narratives of the Public Sphere in the "Democracy Action Plan". *Javnost - The Public*, 31(3), 364–381. <https://doi.org/10.1080/13183222.2024.2382662>.
- 61) GIATOC. (2024). "Cyber-Enabled Crime Poses Significant Risks to South Eastern Europe." *Risk Bulletin* 19. <https://riskbulletins.globalinitiative.net/see-obs-019/01-cyber-enabled-crime-south-eastern-europe.html>.
- 62) Giddens, A. (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Polity Press.
- 63) Global Engagement Center GEC (2020). *GEC special report: Pillars of Russia's disinformation and propaganda ecosystem*. Global Engagement Center. https://2021-2025.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf
- 64) Global Engagement Center (GEC). (2022). *Global Disinformation Trends: Focus on the Western Balkans*. U.S. Department of State.
- 65) Government of the Republic of North Macedonia. (2015). "Груевски во посета на глобалната компанија Хуавеи, презентрани можностите за инвестирање" [PM Gruevski presents investment opportunities in Huawei]. <https://vlada.mk/node/13786?ln=mk>.
- 66) Government of the Republic of North Macedonia. (2017). "Премиерот Заев со менаџментот на Хуавеи на Самитот 16+1: Во Македонија се создадени услови за нови инвестиции и соработка

- на заеднички проекти” [Prime Minister Zaev with Huawei's management at the 16+1 Summit: Conditions for new investments and cooperation on joint projects created in Macedonia]. November 27, 2017. <https://vlada.mk/node/13786?ln=mk>.
- 67) Hedling, E., & Ördén, H. (2025). Disinformation, deterrence and the politics of attribution. *International Affairs*, 101(3), 967–986. <https://doi.org/10.1093/ia/iiaf012>.
- 68) ITU. (2023). *Digital Innovation Profile – North Macedonia*. International Telecommunication Union. <https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2023/Digital%20Innovation%20Profile%20-%20North%20Macedonia.pdf>.
- 69) Juhász, K. (2024). European Union defensive democracy's responses to disinformation. *Journal of Contemporary European Studies*, 32(4), 1075-1094.
- 70) Kaska, K., Beckvard, H., & Minári, T. (2019). *Huawei, 5G and China as a security threat*. NATO Cooperative Cyber Defence Centre of Excellence. <https://www.ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf#page=18.46>
- 71) Kinnvall, C. (2004). Globalization and religious nationalism: Self, identity, and the search for ontological security. *Political Psychology*, 25(5), 741–767.
- 72) Kratochvíl, P., Ditrych, O. & Švec, J. (2025). D6.3 – *Contestation over Truth Regimes: Russia, China and the US digital diplomacy on the Russian invasion of Ukraine*. Reclaim. https://ams.overcastcdn.com/documents/RECLAIM_Contestation_over_Truth_Regimes.pdf.
- 73) Larrabee, F. S. (1994). *The volatility of the Balkans*. RAND Corporation.
- 74) Limitone, Julia. (2019). “Pompeo Slams Huawei: US Won't Partner with Countries That Use Its Technology.” *FOXBusiness*. 2019. <https://www.foxbusiness.com/technology/pompeo-slams-huawei-us-wont-partner-with-countries-that-use-its-technology>.
- 75) Mitzen, J. (2006). Ontological security in world politics: State identity and the security dilemma. *European Journal of International Relations*, 12(3), 341–370.
- 76) Müller, M. (2015). Assemblages and actor-networks: Rethinking socio-material power, politics and space. *Geography Compass*, 9(1), 27–41.
- 77) National AI Platform. (2025). “Serbia Adopts Strategy for the Development of Artificial Intelligence for the Period 2025–2030.” Government of Republic of Serbia. <https://ai.gov.rs/vest/en/1296/serbia-adopts-strategy-for-the-development-of-artificial-intelligence-for-the-period-20252030.php>.
- 78) NATO. (2023). “NATO Team in North Macedonia to Help against Hybrid Attacks.” *North Atlantic Treaty Organization*, March 14, 2023.
- 79) Navarro, J. T., García, L. B., & Oleart, A. (2025). How the EU Counters Disinformation: Journalistic and Regulatory Responses. *Media and Communication*, 13(0). <https://doi.org/10.17645/mac.10551>.
- 80) Noutcheva, G. (2009). Fake, partial and imposed compliance: The limits of the EU's normative power in the Western Balkans. *Journal of European Public Policy*, 16(7), 1065–1084.
- 81) O'Brennan, J. (2014). On the slow and bumpy road to EU membership: The Europeanization of the Western Balkans. *European Foreign Affairs Review*, 19(2), 223–241.
- 82) Ördén, H. (2019). Deferring substance: EU policy and the information threat. *Intelligence and National Security*, 34(3), 421–437. <https://doi.org/10.1080/02684527.2019.1553706>.
- 83) Ördén, H. & Pamment, J. (2021), *What is so foreign about foreign influence operations?*, Carnegie Endowment for International Peace.

- 84) Pamment, J., Fjällhed, A., Szepesi, V., & Jonsson, O. (2022). *The role of the EU in countering disinformation: Policy gaps and future directions*. Swedish Civil Contingencies Agency (MSB).
- 85) Pamment, James, et al. (2022). *Countering Foreign Interference: An EU Handbook for Practice*. European External Action Service.
- 86) Proto, L., Lamoso-González, P., & García, L. B. (2025). The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight. *Media and Communication*, 13. <https://doi.org/10.17645/mac.9474>
- 87) RCC (Regional Cooperation Council). n.d. "Digital Economy". https://www.rcc.int/priority_areas/56/digital-economy.
- 88) Ruge, M., & Vladislavljev, S. (2020). Serbia's 5G deal with Washington: The art of muddling through. *European Council on Foreign Relations*. https://ecfr.eu/article/commentary_serbias_5g_deal_with_washington_the_art_of_muddling_throug_h/
- 89) Rumelili, B. (2015). Identity and desecuritisation: The pitfalls of conflating ontological and physical security. *Journal of International Relations and Development*, 18(1), 52–74.
- 90) Rupnik, J. (2011). The Balkans as a European question. In *The Western Balkans and the EU: 'The hour of Europe'* (Chaillot Paper No. 126). EU Institute for Security Studies.
- 91) Salihu, G. (2023). The US–China 5G race in Europe's Western Balkans. In J. Berghofer et al. (Eds.), *The implications of emerging technologies in the Euro-Atlantic space* (pp. 43–55). Springer. https://doi.org/10.1007/978-3-031-24673-9_3
- 92) Steele, B. J. (2008). *Ontological Security in International Relations: Self-Identity and the IR State*. Routledge.
- 93) The National Agency for Information Society. (n.d.) "Digital Agenda of Albania 2022–2026." Geneva Internet Platform. <https://dig.watch/resource/digital-agenda-of-albania-2022-2026>.
- 94) Umbach, F. (2020). *EU policies on Huawei and 5G wireless networks: Economic-technological opportunities vs cybersecurity risks* (S. Rajaratnam School of International Studies Working Paper No. 332). Nanyang Technological University. <https://hdl.handle.net/10356/146478>
- 95) Vladeva, G. (2014). Enlargement fatigue in the Western Balkans: The role of domestic politics. *European View*, 13(1), 22–30.
- 96) Vladislavljev, S. (2021). *China's 'Digital Silk Road' enters the WBs*. Association for International Affairs; China Observers in Central and Eastern Europe – CHOICE. https://chinaobservers.eu/wp-content/uploads/2021/06/CHOICE_policy-paper_digital-silk-road_A4_web_04.pdf
- 97) WBIF (Western Balkans Investment Fund). n.d. "Digital Future." <https://www.wbif.eu/sectors/digital-infrastructure>.
- 98) Zartman, I. W. (2005). *Cowardly lions: Missed opportunities to prevent deadly conflict and state collapse*. Lynne Rienner Publishers.
- 99) Zhang, K. H. (2024). Geoeconomics of US-China tech rivalry and industrial policy. *Asia and the Global Economy*, 4(2), 100098. <https://doi.org/10.1016/j.aqlobe.2024.100098>