

The EU’s Struggle Against Strategic Disinformation during the COVID Pandemic: An Assemblage Approach

ONDREJ DITRYCH	European Union Institute for Security Studies (EUISS), France
E-MAIL	ondrej.ditrych@iss.europa.eu
JAKUB EBERLE	Institute of International Relations Prague, Czechia
E-MAIL	eberle@iir.cz
PETR KRATOCHVÍL	Institute of International Relations Prague, Czechia
E-MAIL	kratochvil@iir.cz
LINDA MONSEES	Institute of International Relations Prague, Czechia
E-MAIL	monsees@iir.cz
ABSTRACT	The Covid pandemic was a pivotal episode in the evolution of the European Union’s response to strategic disinformation. This article deploys assemblage theory to advance a critical, interpretive understanding of truth contestation as an increasingly salient dimension of geopolitical conflict – one in which foreign actors seek to undermine the epistemic foundations of rival political communities. Strategic disinformation assemblages, conceived as foundationless, emergent, and heterogeneous composites of human and nonhuman elements, exploited pandemic-induced uncertainty to challenge public trust in EU institutions, health authorities, and countermeasures. In response, the counterdisinformation assemblage evolved at both EU and member-state levels. Through comparative case studies of France and the Czech Republic, the article demonstrates that even under a shared securitisation logic, counterdisinformation practices could diverge significantly: France pursued a state-centric model emphasising digital sovereignty and institutional capacity, while the Czech Republic exhibited a more diffuse, civil-society-driven approach that was marked nonetheless by a notable discursive militarisation.
KEYWORDS	disinformation, covid, assemblage, France, Czech Republic
DOI	https://doi.org/10.32422/cjir.1944
PUBLISHED ONLINE	11 September, 2026

INTRODUCTION

Truth contestation is an increasingly salient dimension of global geopolitical conflicts. Safeguarding the integrity of the information space in the face of the evolving challenge of foreign information manipulation and interference remains an important political rationality behind recent initiatives such as the European Democracy Shield (EUROPEAN COMMISSION, 2025). Globally, countering disinformation poses risks for independent journalism and contribute to authoritarian consolidation (CF. LIM & BRADSHAW, 2023). The research on disinformation, particularly its critical strand focused on exploring political impacts of its production and dissemination but also strategies of countering disinformation, thus maintains its practical relevance and purchase.

The Covid pandemic is a key episode in the forming of the set of rationalities, technologies and practices of the EU's countering of strategic disinformation – its counterdisinformation *assemblage*. Many of the disinformation narratives circulated in the EU during Covid were unorchestrated responses to uncertainty. However, strategic disinformation campaigns enacted by foreign actors also considerably informed the “infodemic” by producing or amplifying claims that carried the potential to undermine trust in public authorities and policies. These ranged from bizarre conspiracy theories, such as those about vaccines that supposedly turn people into monkeys (SKY NEWS, 2021) and claims that the virus was a biological weapon masterminded to create a totalitarian rule by global elites, to falsehoods about the effectiveness of counterpandemic measures put in place by the member states.

This article offers a conceptually innovative reading of the truth contestation surrounding the Covid pandemic. Deploying the concept of assemblage, it advances interpretive research on strategic disinformation – for recent contributions to this research, see (E.G., STARBIRD, 2019; STARBIRD, ARIF & WILSON, 2019; URAKAMI ET AL., 2022; PASQUETTO ET AL., 2022; HAMELEERS, 2024; ISKANDEROVA, 2024; TRIPODI, GARCIA & MARWICK, 2024; MALHOTRA ET AL., 2025). It sheds light on the modalities of contestation in global politics concerned with the epistemic foundations (“truth regimes”) of societies on which certain economies of power are erected. In particular, it focuses in detail on the evolution of the EU's counterdisinformation assemblage, conceived as one historically specific articulation of a security assemblage, as the EU and its member

states were confronted with a shifting challenge of strategic propaganda and disinformation – understood by the EU as false or misleading content produced and disseminated with the intent to deceive or seek economic or political gains (COUNCIL OF THE EUROPEAN UNION, UNDATED) – during the pandemic. In two detailed case studies of the Czech Republic and France, respectively, the article shows how adaptation to this evolving challenge can take plural pathways depending on social and cultural contexts and constellations of actors' interests and strategies.

The argument proceeds as follows. In the first section, a critical survey of the scholarly literature on Covid and disinformation is presented. It identifies three distinct streams: the descriptive, analytical and critical ones. Then we explain how assemblage theory can be deployed in critical disinformation research to advance an interpretive understanding of contestation over truth in which geopolitical conflict reaches to the epistemic foundations of the adversary's societies, and discuss the evolution of the EU's counterdisinformation assemblage in this framework. The assemblage theory, which conceives practices as foundationless, emergent (rather than administered from a "centre"), complex and heterogenous, offers itself as a productive perspective for better understanding this contestation and track the dynamic and relational construction of this counterdisinformation assemblage. Drawing on a "polemic" understanding of contestation over truth as an increasingly significant dimension of contestation in contemporary global politics (DITRYCH, 2026), it is situated in a broader field of formation of assemblages as sociomaterial structures. One kind of these mutating *disinformation* assemblages combines bots, algorithms and infrastructures with human agency to collaboratively produce, share and process disinformation; another kind is designed to counter these disinformation machines: it concerns counterdisinformation assemblages affixed to maintain or restore the "interiorisation function" of the state by protecting its epistemic cores. Finally, the article presents two detailed empirical case studies tracing the evolution of the counterdisinformation practice during the pandemic.

DISINFORMATION AND THE PANDEMIC: A CRITICAL LITERATURE SURVEY

The Covid pandemic, in addition to the 2016 US-election and the

Brexit referendum, has been considered as a main episode in the evolution of (counter-)disinformation assemblages. Scholars from a variety of fields such as media studies, sociology, law and political science have examined the spread and impact of disinformation, and possible countermeasures against it (TANDOC ET AL., 2017; CONRAD & NEWMAN, 2024; SIMION, 2023; BASTICK, 2021; VESE, 2022; MONSEES, 2023; POLLETTA & CALLAHAN, 2017). In this section we survey the literature, identifying three strands of research: *descriptive research* that is mostly interested in taxonomies of disinformation, a more *analytical research* which is interested in the consequences of disinformation and attempts at its regulation, and a more *critical research* that often draws inspiration from poststructuralist or critical theoretical lines of social inquiry. The value of this last strand, we propose, lies in particular in its opening new venues for examining the impact of the production, dissemination and countering of disinformation on the political life of societies. Furthermore, it forms a vantage point from which the epistemic dimension of the rising global geopolitical contestation (EKMAN & EVERTS, 2024) that concerns truth regimes underpinning the exercise of power, can be productively interrogated.

The descriptive research is concerned with the difficult task of finding appropriate definitions for the different versions of mis- and disinformation and how we can make sense of it in the context of EU policies and politics (BOUZA GARCIA & OLEART, 2024). An important distinction lies between false information that is aimed at causing harm and that which is not (WARDLE & DERAKHSHAN, 2017). This distinction is necessary in order to distinguish between intentional distribution of false information and journalistic or technical mistakes. It is highlighted in, among other sources, the EU definition of 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” (CITED BY KACHELMANN & REINERS, 2023, P. 14), which we therefore consider useful for orienting our own analysis below.

In the analytical research stream, social sciences have been pivotal in expanding our descriptive knowledge about the spread, sources and impact of disinformation and how it impacts public discourse, elections and polarisation (BAK, WALTER & BECHMANN, 2023; CZERNIAK ET AL., 2023; GALLOTTI ET AL., 2020). More recent literature in this stream focuses on the EU’s attempts to govern

disinformation, especially in the wake of the Covid pandemic (HARRISON 2021; STORENG & DE BENGUY PUYVALLÉE, 2021, P. 1490). The key finding here is “a high level of engagement [by the EU] in its fight against disinformation, driven by serious concerns of the risk of online disinformation” (SAURWEIN & SPENCER-SMITH, 2020, P. 7), especially in the context of elections. The main countermeasures pointed out by the literature include more voluntary based measures such as the fact-checking and self-regulation performed by platforms (IBID., P. 11) but also direct governmental interventions such as content removal and criminal sanctions (HELM & NASU, 2021). Overall, disinformation is considered a *problem*, for example because it increases resentment against migrants and foreigners and fosters populist politics which use disinformation to pursue their own policy goals (CONRAD, 2022).

More specifically, in the context of the pandemic, the term “infodemic”, first introduced by the World Health Organisation (WHO), is used to capture the relationship between disinformation and a broader transformation of the public sphere (GALLOTTI ET AL., 2020; HEISS ET AL., 2021; VÉRITER, BJOLA & KOOPS, 2020; RADU, 2020). However, this term is problematic as it suggests that disinformation is *just like* a virus, spreading uncontrollably around the globe. This ignores that the impact of fake news might be much more diffuse and lie not only in the falsehood of the story as such but in a priori structural conditions (e.g., antidemocratic, racist and sexist ones). The analytical research often claims that singular events such as the 2016 U.S. election or Covid led to a dramatic increase in disinformation (HEISS ET AL., 2021, P. 1) – and that this necessitates a strong response. However, this often neglects that disinformation has a much longer history (TANDOC, LIM & LING, P. 2017) and that many EU policies following Covid can be seen as extensions of earlier processes rather than radical ruptures (CARRAPICO & FARRAND, 2020). In sum, this strand of research offers a more analytical understanding of disinformation, but it falls short in understanding the broader societal and political context.

The last strand of research is more concerned with the “chilling effects” (VESE, 2022; HOBOKEN & Ó FATHAIGH 2021) that the countermeasures might have on the freedom of expression and other constitutional liberties (PEUKERT, 2024). According to this scholarship, some measures taken by the EU (and its member states) may be a cause of concern, as “the pandemic has encouraged strict government policies, which, acting under the threat of loss of life, have passed particularly invasive human rights laws to

manage the risks of online disinformation” (VESE 2022, PP. 483–484). While the trend towards overregulation and overreach into civil rights and liberties in responses to disinformation has been in place for some time according to these arguments, it further accelerated during the pandemic (HOBOKEN & Ó FATHAIGH, 2021, P. 10; VESE, 2022, P. 499).

This critical literature is concerned less with the immediate effects of and responses to disinformation but uses the debates around disinformation as a springboard for an analysis of their broader societal effects and (mostly) unintended consequences (CASERO-RIPOLLÉS, TUÑÓN & BOUZA-GARCÍA, 2023; SAURWEIN & SPENCER-SMITH, 2020; STORENG & DE BENGY PUYVALLÉE, 2021). Building on concepts such as securitisation, governmentality or feminist thoughts, research in this stream link disinformation and the EU responses to wider traditions of sociological analyses of security (RØD, PURSIAINEN & EKLUND, 2025; AGAJANIAN & MORAN, 2025; MONSEES, 2023). For example, grounding their argument in securitisation theory, Casero-Ripollés et al. (2023) suggest that the EU has increasingly viewed disinformation through a securitised, geopolitical lens (SEE ALSO EBERLE & DANIEL, 2023). Through this “geopolitical logic”, the EU “conceives disinformation as a weapon used by foreign rivals or enemies to exploit the vulnerability of democratic publics to manipulation and interference” (CASERO-RIPOLLÉS, TUÑÓN & BOUZA-GARCÍA, 2023, P. 3). Other authors such as Hoboken and Ó Fatnaigh (2021) then point out potential problems with the militarisation of EU disinformation policies – such as that invoking the notion of emergency may hamper democratic debates about alternative solutions to the (real) problem.

Beyond this argument, grounded in the standard securitisation theory, one also finds in this stream explorations of fundamental reconfigurations of power and subjectivity that are at play in debates and policies concerning disinformation. Some of these highlight the networked nature of agency and accountability, e.g. by conceptualising disinformation as a “socio-technological assemblage of risk” (SAURWEIN & SPENCER-SMITH, 2020). This perspective foregrounds the complex and multifaceted nature of the digital environment in which the production, circulation and consumption of disinformation occur through “a combination of platform design, algorithms, human factors and political and commercial incentives” (IBID., P. 834). This strand of research thus helps us to see how disinformation – and countering it – through a multiplicity of actors can become a means of reshaping the relationship between the state, citizens and media and

ultimately our ideas about “truth” in the public sphere (SEE HAYWARD, 2025). In this article we build on these insights and expand them by using the concept of assemblage in order to deepen our critical understanding of the effects of disinformation.

DEPLOYING ASSEMBLAGE THEORY IN CRITICAL DISINFORMATION RESEARCH

Building on this last line of inquiry, in this article we advance the critical interpretive understanding of disinformation and countering it. We do so by focusing attention on the hybrid nature of contestation in global politics, where epistemic foundations (“truth regimes”) of political communities increasingly become an object of conflict. These epistemic foundations, we argue, are indispensable for exercise of political power. As they are more easily within reach because of technological progress yielding digital communication technologies and facilitating the creation of new, deterritorialised fields of contestation, their disruption is not just a strategy of domestic political dissent but also of geopolitical conflict – and is securitised as such by state security apparatuses that evolve to face it as a security problem. Assemblage theory, which conceives these polemic practices by collective agents in global politics as foundationless, emergent, complex and heterogenous, is a useful lens for better understanding the nature of this contestation, so far undertheorised in the interpretive disinformation research, over the fundamentally political question of what constitute key and irrefutable truths enabling the exercise of power in political communities (CF. FOUCAULT 2000) and, from a liberal, problem-solving perspective (ADLER & DRIESCHOVA, 2021).

Drawing on a number of notable contributions to the thinking about global politics and security through assemblages (AMONG OTHERS, ONG & COLLIER, 2005; SASSEN, 2006; MCFARLANE, 2009; ABRAHAMSEN & WILLIAMS, 2009; ACUTO & CURTIS, 2014; DITTMER, 2013; MÜLLER, 2015; DOUCET, 2016; ARADAU, 2017; BUEGER, 2017; LOPEZ-LUCIA & DE ALMAGRO, 2023) and its continental theory inspirations, we understand an assemblage as a heterogenous, decentred and fragmentary composite of diverse elements, including agents, things, discourses, rules and institutions, affixed for some strategic purpose (SEE, IN PARTICULAR, DELEUZE & GUATTARI, 1987; DELEUZE, 1992; MARCUS & SAKA, 2006; ACUTO & CURTIS, 2014; MÜLLER, 2015; DITTMER, 2017). Through the assemblage theory lens, the dimension of contestation in global politics that takes epistemic foundations of political communities

as its object can be understood as a polemic relationship (cf. DITRYCH, 2026) of two distinct types of assemblage (which may take various specific forms): the strategic *disinformation assemblage* and the *counterdisinformation assemblage*. The latter branched out from the security assemblages as it recomposes itself in response to the threat “picture” it takes by using previous and developing new forms of security knowledge.

Strategic disinformation assemblages, from this perspective, can be conceived as makeshift composites arranged and deployed with a strategic intent by external actors in the context of the geopolitical contestation to challenge fundamental truth regimes with another polity. They feature both truth formation and truth contestation tactics, which are strategically deployed to disrupt the shared sense of reality, “common sense” and basic narratives and sentiments through which facts are made intelligible; and reshape the terrain on which deliberation in democratic societies take place. While their content is subject to metamorphosis – in processes of appropriation, recoding and repurposing – this disruption function enacted by collaboration on composition, distribution and circulation, is the trademark of the disinformation assemblage. By far not all disinformation circulated within western democracies can be traced to Russia and/or China or other adversarial outside actors, or in any way linked to the geopolitical contestation. Even disinformation produced collectively can be a result of a coordinated effort without foreign interference – while the domestic disinformation assemblages may be borrowing “pieces of code” from available transnational pools. The strategic disinformation assemblages discussed here are those that can exploit domestic controversies but are linked to one particular and increasingly more pronounced dimension of geopolitical contestation that qualitatively differs from the more conventional propaganda: efforts to undermine the epistemic foundations of rivals and adversaries’ political communities and disrupt the exercise of power within them. In the conditions of the information revolution, one of the key landscapes of contestation is social media “platforms”. Far from being contained communication spaces, these platforms are a complex field of contestation where truth regimes are (re-) produced and challenged (see, for example, COSENTINO, 2020; AYTAÇ, 2024; VALASKIVI & ROBERTSON, 2022).

It is against this challenge that counterdisinformation assemblages emerge – they are assembled to counter strategic disinformation and to

maintain and restore the space in which government can be performed. Their declared objective is the removal of insecurity and restoring the “interiorisation function” of the state (DELEUZE & GUATARRI, 1987). This is a function that produces a space in which government can be exercised by means of appropriation, purification and externalisation of difference. Responding to the securitisation of the epistemic challenge, counterdisinformation assemblages constitute particular formations of broader state security assemblages as these evolve over time, repacking and repurposing elements from previous composites (drawn, for example, from the counterterrorism assemblage) – and, when confronting the contestation on social media, combining practices of sovereignty (prohibition), surveillance (discipline) and governmentality in new hybrid composites.

The potential of assemblage theory to interpret strategic disinformation is anchored in the specific understanding of the disinformation and counterdisinformation apparatuses that populate global politics as a field of contestation. Strategic disinformation assemblages are foundationless. They have no fixed essence and, unlike more conventional, ideologically grounded propaganda machines, are defined by no singular, totalising forms of knowledge – while potentially borrowing from multiple ones without a pressure for overall coherence. They are also emergent. They are made up of elements, their unity achieved only by their functioning together in a temporary symbiosis, and always makeshift, transforming over time in a strategic yet not necessarily orchestrated morphogenesis. Finally, they are complex and heterogenous, with components drawn from both human and nonhuman estates, involving human agents, material artifacts and infrastructures that become linked but also remain autonomous (DE LANDA, 2006). The counterdisinformation assemblages might seem to be more “founded” yet they are not necessarily aligned with the epistemic foundations they are tasked to protect – and as a matter of fact, these foundations are also not immutable as they are rather defined by their *function*: that of maintaining consent with the exercise of a political power productive not only of certain discursive orders, but also of certain sociopolitical hierarchies. Like strategic disinformation assemblages, while following a certain line of force, the counterdisinformation assemblages are also emergent; and like the former, they are complex composites of heterogeneous elements – for example, both “state” and “nonstate” elements.

Mobilising the assemblage theory for use in disinformation research may benefit the interpretive study of disinformation by exploring how strategic disinformation and the security practice of countering it operate across spatial and temporal contexts. The perspective can moreover shed light on how the polemic relationship between disinformation production and dissemination practices on one hand, and protecting the securitised epistemic foundations of the state on the other, functions as a field of contestation in global politics. Unlike other concepts such as the network, for applications of network theory to the study of disinformation see (E.G., DELLA LENA, 2024; SMITH ET AL., 2021; AZZIMONTI & FERNANDES, 2023), which offer a useful methodological toolbox for exploring linkages between elements and also pointing out/to social associations' emergent and complex properties, assemblage theory focuses the analytical gaze on social production and the exercise of power. This exercise is enacted in a field of formation where (in our case, strategic *disinformation* and *counterdisinformation*) assemblages emerge in a relationship of functional complementarity due to their disruption / maintenance objective related to established truth regimes constitutive of power relations. Furthermore, the wide array of agents affixed together in an assemblage can serve to balance the reductionist technological determinism in the disinformation research with its emphasis on communication technologies or algorithmic structurings that push into the background human habitus and dispositions as well as social and cultural contexts in which (dis-)information is collaboratively produced, shared and processed by human agents. Finally, the emphasis on the foundationless character of assemblages does not make the disinformation research removed from or immune to the polarisation and politicisation that define it at present (CF. PASQUETTO, LIM & BRADSHAW, 2024). However, it does provide a vantage point from which contestation in global politics can be explored and analysed without a commitment to one particular truth (regime) or another.

DISINFORMATION AMIDST COVID: SECURITISATION AND ADAPTATION

The Covid pandemic as a global crisis created a new dynamic for the evolution of disinformation and counterdisinformation assemblages. The former ones, which had the epistemic foundations of liberal societies as their target, adapted to the new circumstances in which the global health crisis translated into domestic states of exception authorised and sustained

by biopolitical concerns over public health (SEE ALSO RYCHNOVSKÁ, 2021; ELBE, 2022; ELBE ET AL., 2023). They amplified and exploited the related controversies – and, in the view of the EU and its member states, exploited “gaps of knowledge” “among EU populations, in other words the epistemic crisis caused by the pandemic resulting from individuals’ confinement as well as the irregularity of the pandemic as a (hyper-)event (TACKLING THE COVID-19, 2020). The narratives they produced and disseminated through the material content circulation infrastructures they comprised (CF. BRADSHAW & NARDIS, 2022) addressed Russia and China’s roles in the crisis, public trust in the EU’s member states, and dominant truth claims related to the virus’s origin and the effectiveness of the adopted countermeasures to limit the spread and health effects of the pandemic – such as the isolation policies or the vaccines.

How the EU counterdisinformation assemblage problematised the threat the disinformation machines built around China and Russia posed for European security is well described in the EEAS public situation reports. The first set of descriptions contained there portrays the disinformation assemblages, as seen by the EU securitising gaze, as forming a distinct basic discourse of identity and difference. In the disinformation narratives produced and disseminated in these assemblages, Russia and China were constructed as responsible, altruistic powers that were (allegedly) ready to come to others’ rescue rather than as actors playing a role in the virus’s conception and spread (EEAS, 2020A, 2020B, 2020C, 2020D). They were also presented as internally efficient in containing the disease – in China’s case, for example, by virtue of its centralised governance model (EEAS, 2020D). Conversely, the EU was portrayed as selfish and as betraying its own values when confronted with Covid. When discussing the member states, the narratives combined a more conventional and ideological propaganda with disinformation to “support” this narrative identity construction. They presented them as decayed and ready to collapse, or alternatively as deliberately turning into “fascist hygiene dictatorships” (IBID.) that heralded the end of the liberal world – including by virtue of the forced but fake “vaccinations” in which controlling nanochips, toxins, or DNA-altering proteins were implanted into bodies of the populace (EEAS, 2020A, 2020C).

In addition to these conspiracy narratives, the disseminated disinformation furthermore comprehensively addressed countermeasures enacted or advocated by public authorities in the EU. This set of narratives comprised coordinated false health information designed to amplify the

negative sentiments against the lockdown measures in the EU (EEAS 2020E) as well as those related to the vaccines. Targeting the trust of the public in the official information in the conditions of uncertainty and crisis, these narratives countered the member states' appeals (or demands) for citizens to get vaccinated and thus check the spread of the disease by asserting that the vaccines were unnecessary, ineffective, risky or even harmful. A testimony to the diversity (and occasional incoherence) of the content produced by the disinformation assemblages, these narratives, intended to undermine the knowledge supporting the vaccinations whose use was advised or ordered by public authorities, were compounded by massive advertisements for "efficient" and "highly desired" Russian and Chinese vaccines that were intended to increase their purchases while undermining the trust in the western vaccines – such as the "monkey vaccine" produced by AstraZeneca (IBID.).

The EU's counterdisinformation assemblage, as a branch of the more general composite security assemblage acting as an apparatus for "management of unease" (BIGO, 2002) at the member state and institutional levels, was adapting to this evolving challenge that continued to be conceived under the hybrid threat rubric. This can be seen as an extension of a process traced back to Russia's annexation of Crimea (2014), after which "hybrid threats" – a wide array of phenomena compressed in a single security *problematique* – became more salient in the security field. To counter the strategic disinformation assemblages, which were conceived as deterritorialised and as undermining, delegitimising and destabilising democratic societies (JOINT COMMUNICATION, 2018; EEAS, 2015), challenging their core values and principles, weakening social cohesion and dividing populations, and removing trust in EU institutions and member states' governments in the conditions of corrupt communication and a (hyper-)polarisation of the political debate, new means of intervention were called for to restore the *inside/outside* boundaries – and so restabilise the (sovereign) domestic order through inscriptions of a stable sense of collective identity (EUROPEAN SECURITY UNION STRATEGY, 2020; JOINT COMMUNICATION, 2016).

This call to arms became more forceful with the widening of the frame of disinformation as a core security problem. The early focus on competing interpretations of particular events such as Russia's first aggression against Ukraine (2014–) and its later threats of electoral interference shifted to the undermining of democratic foundations and public health concerns by

means of “systematic information and manipulation and disinformation by the Kremlin” as a “significant and direct threat to the Union’s public order and security” (EUROPEAN COUNCIL, 2022). The Covid pandemic was a key event facilitating this shift. Hand in hand with the volume of disinformation on the causes, the nature of the disease, its treatment and responses by member states’ public authorities, a *public health-security nexus* was established, including by means of the introduction of terms such as *infodemic* that “[feed] on people’s most basic anxieties” (TACKLING THE COVID-19, 2020). The challenge of the infodemic to the epistemic foundations of European polities through its subversion of the knowledge about the epidemic and its broader challenge to their bureaucratic rationality were conceived as a cause of individual “risky behaviours” – from not washing one’s hands to refusing to isolate or wear masks, or be vaccinated – and of an undermining of the trust in democratic government (IBID.).

This securitisation process (for a critical analysis of it, (SEE VERITER, 2025)) was an impetus for an enlargement of the countersecurity assemblage but also a modification of its basic political rationality and corresponding technologies. As a result, security responsibilities were becoming more distributed. Member states’ security apparatuses and European institutions but also corporations, NGOs (“watchdogs”) and individuals were being enlisted in the “whole-of-society” effort to combat disinformation. Private corporations were pressured to take responsibility for “content moderation” (EUROPEAN DEMOCRACY ACTION PLAN, 2020; EUROPEAN COMMISSION, 2022) and were (often reluctant) targets of regulatory practice. They were required to promote “authoritative content” from national and international health agencies, inform users when they interacted with disinformation, report instances of social media manipulations or coordinated “inauthentic behaviour”, or demonetise the dissemination of disinformation (TACKLING THE COVID-19, 2020; EUROPEAN COMMISSION, 2022). Nonetheless, their actions were deemed insufficient: the EU security apparatus continued to problematise what it considered the providers’ failure to protect the public interest (EEAS, 2020C) on one of the key platforms of contestation (see above) by continuing to monetise disinformation and conspiracy theories related to Covid, and resisting efforts to make digital identities more transparent (making it “nearly impossible to detect and attribute covert behaviour” ((EEAS, 2020B)) or the content algorithms (IBID.)). The verification (“fact-checking”) practice was another way to enlist nonstate actors in efforts to indirectly counter the epistemic challenge of the disinformation and “set

things right” through a collaboration between NGOs, media, independent researchers, and platform providers.¹ Furthermore, individuals too were increasingly being expected to do their part in countering disinformation. Their faculties (“critical thinking”) became a target in efforts to increase individual resilience.²

This broad involvement of many agents – outlined if not always successfully enacted, as the case studies below show – correlated with the generalised and capillary understanding of the threat of the strategic disinformation permeating and corroding European societies. It was also facilitated by the fact that the push for more punitive and prohibitionist approaches was constrained, even in the conditions of exceptional politics, by law, as well as by the complex relationship of mutual enhancement but also frictions between (“resurgent”) sovereignty and neoliberal governmentality. As a result, the prohibition and punishment rationalities enabled by the exceptional politics were countered by approaches more focused on individualisation and responsabilisation. This contributed to the development of many internal varieties within the EU counterdisinformation assemblage. The following section explores in more detail two of these varieties at the member state levels, namely those of France and the Czech Republic.

VARIED MOVEMENTS

The cases of France and the Czech Republic show the varied evolution of different member states’ elements of the EU counterdisinformation assemblage during the pandemic. Each represents a member state of a different size, history and geography. At the same time, in both, strategic disinformation and propaganda were clearly securitised before and during the pandemic, and the counterdisinformation assemblage evolved as a result of the securitisation process.

In both cases, the securitisation process took place in the broader EU context, and a part of the solution has been sought at the EU level. That said, the case studies show how the same securitisation process, even in this shared context, could lead to different outcomes. The shaping of the counterdisinformation assemblage to counter disinformation in France had a strong state-centric logic and, as a consequence, was shared by the desire to establish digital sovereignty. In contrast, in the Czech case the

constitution of the counterdisinformation practice was less directional and more diffused from the outset, suggesting how a securitisation driven by the state might not be the only or even the dominant form of securitisation. The absence of a strong centralised push on behalf of the state institutions was offset by a coalition of different actors within the assemblage. The case shows how in response to a perceived inaction or inefficiency of the government, nonstate actors, including think tanks, media and private companies, can utilise their networks and resources to mainstream conceptions of security and the related truth regimes, sometimes in close cooperation with individual actors from within the state institutions. However, the pre-Covid investment in the agenda by elements of the governmental security apparatus also meant that, ironically, the countering of disinformation was militarised and conceived in terms of the discourse of (hybrid) war. This framing would then be adopted also by the nonstate actors involved in the counterdisinformation assemblage, and sustained by their subjectivation as “elves” fighting malign “trolls” in an atavism-generating instance of a Tolkien-inspired imaginary infusing present-day politics.

FRANCE

The main trigger of the counter-disinformation policy in France before Covid was the electoral interference by Russia. After the 2017 presidential election that witnessed various disinformation campaigns, including the “Macron Leaks”,³ the law against the manipulation of information (*ASSEMBLÉE NATIONALE, 2018*) was passed to protect the integrity of the elections. An interministerial committee to counter information manipulation was set up and it brought together the relevant ministries and intelligence services.

Under the law, candidates and political parties could now appeal to a court to order a removal of a massive and artificial circulation of false information in the three months before an election.⁴ The law made its violations punishable by a prison sentence of up to 12 months and a fine of EUR 75,000 as it outlawed behaviours that were conducive to dissemination of disinformation, for example a failure to disclose a financial amount that was provided to a media source in exchange for its publishing certain content. Furthermore, the Supreme Council for Audiovisual Media (*Le Conseil supérieur de l'audiovisuel, CSA*) could now suspend broadcasting

or the provision of digital services controlled or under the influence of a foreign state if it or they intentionally disseminated disinformation that was likely to manipulate electoral results – a response to the growing audiences of the Russian state media RT and Sputnik as well as the inadequate regulation of the online content they produced, and the understanding of this as a security concern.⁵

This securitisation process took place against the backdrop of framing in security terms the emergence of the global digital space, which, in the words of the then Foreign Minister Jean-Yves Le Drian, “posed new risks of alienation of individuals and societies” (SOCIÉTÉS CIVILES, 2018). As a result, the internet had to be regulated. This, President Macron stated at the time, was “[a] *sine qua non* condition for a free, open and secure internet, as envisioned by its founding fathers” (FIORENTINO, 2018). However, while the law was also criticised for allegedly giving the government the power to censor the information space and monopolise and police the truth (GUILLAUME, 2019), it remained more on the *governmentality* than the sovereignty side: not prohibiting or coercing, but rather establishing a duty of cooperation for social media companies that obligates them to disclose the sources of funded political content, implement faster removal systems for disinformation, provide users with better mechanisms to report suspicious or false content, and offer more transparency, but without giving the government effective means for the enforcement of the law.

The key declared political rationale of the counterdisinformation assemblage was the need to preserve “information integrity”. The most important state institutions involved in this effort were the Ministry of Foreign Affairs, the Ministry of the Interior and the Ministry for Digital Affairs, as well as the DGSE (civil intelligence), the National Cybersecurity Agency (ANSSI) attached to the SGDSN (the General Secretariat for Defence and National Security within the Prime Minister’s Office), and the French Data Protection Authority (CNIL). The strategic communications coordinated through the Government Information Service (Service d’information ud Gouvernement, SIG) at the Prime Minister’s Office should also be seen as forming a part of the counterdisinformation assemblage. Furthermore, from the outset, a number of media literacy and fact-checking initiatives were involved, either through civil society entities or as official media projects. *AFP Factuel* was an example of the latter.

With the advent of Covid came disinformation and conspiratorial narratives in the French public information space that were aimed at disrupting mainstream truth regimes concerning the origin of the virus and the countermeasures to it (lockdowns, mandated vaccination, the *pass sanitaire*, which was seen as an infringement of personal freedom, mask mandates, state support to alleviate the economic impact of the lockdowns and other restrictive measures). They further sought to instil doubts about the public authorities' general sense of direction and ability to respond to the pandemic – or the timing of their response (e.g. a wave of online content hashtagged *#IlsSavaient*, “they knew [... and did nothing]”; see (ZBIEREN, 2020)) – as well as to, alternatively, frame Covid as a fabricated health crisis designed to control the population. According to these conspiratorial narratives, the virus either did not exist at all, or was intentionally disseminated by the government, for example with the use of 5G towers (which were also “theorised” as suppressing immune systems). Later, Covid vaccines also were framed as material artifacts of control that alter the recipients' DNA or insert microchips into their blood stream.

Actors linked to both Russia and China amplified the locally produced disinformation, and ensured the rapid spread of controversy-stirring content that posed challenges to the knowledge produced to support the government's actions or contributed to forming the public opinion that the government was overreaching and/or failing to address the health crisis. Even before the full-scale invasion of Ukraine, Russia was considered as a key state strategic disinformation actor. According to French governmental statements, Russia was attacking France as well as other democratic states through an “enterprise of massive destabilisation” and using “information and interference manoeuvres” (FAUROUX, 2024). Initially, a particular attention was paid to RT and Sputnik, which could be clearly identified as vehicles of strategic disinformation due to their uncontested relationship to the Russian state. However, later other tactics in the Kremlin playbook, including forgeries and blending factual reporting with fake news on social media platforms, were problematised. As a part of the strategy to counter Russia's strategic disinformation, the government publicised campaigns such as Portal Kombat and Matrioshka (2024) and *RRN/Dopplegänger* (2023) and directly attributed them to Russia.⁶ In comparison, China received less attention – despite, for example, a widely publicised report by IRSEM, the Defence Ministry think tank (CHARON & JEANGÈNE VILMER, 2021), and public information about the Chinese Infektion

2.0 disinformation campaign, which advanced the conspiracy narrative that Covid first appeared at a U.S. military base (GUIBERT & PEDROLETTI, 2021).

The adaptation of the counterdisinformation apparatus during Covid took both a legal and an institutional form. Disinformation related to the pandemic, now seen as posing a threat to public health, and the “communication wars” waged by Russia and China, were the key themes of the securitisation narratives underlying these changes (SÉNAT, 2020). The legislative adaptation consisted in the adoption of the law on the fight against hate speech, or the “Avia Law” (2020). The draft law stipulated that social media platforms had to either remove “manifestly illegal” content that was reported to them or be fined up to 4% of their global revenues in case of their noncooperation (CF. BADOUARD, 2020). However, the draft was significantly moderated already during the parliamentary procedure. Then the core provisions forcing the platform providers to remove content were struck down by the Constitutional Court. Therefore, the only new significant obligation for the social platform providers imposed by the law was the duty to simplify the reporting process.

After the failure of the ambitious regulatory efforts, the focus of the adaptation efforts turned to institutions. First, the task force “Honfleur” was created to detect and analyse information destabilisation efforts. In 2021, building on the Honfleur model, a new state service, Viginum, which was attached to the SGDSN, was created to protect against foreign digital interference. Doubling down on the information environment control – even without the strong legal framework that the government failed to put in place – Viginum was tasked to specifically trace and debunk malicious content on digital platforms that involves foreign powers.^[i] The agency’s core mission was therefore to maintain the internalisation function of the state by marking, as fast and reliably as possible, foreign (“outside”) sources of disinformation and mechanisms of its amplification and mass distribution. Russia and China, and also Türkiye, were most often mentioned as the relevant foreign powers in this respect in the public debate at this time – in the case of Russia, this was also connected with its earlier attempt at electoral interference (MATHEVON, 2021; COHEN, 2021). Furthermore, Arcom (Autorité de régulation de la communication audiovisuelle et numérique) was created in 2022 as a public authority that merged the CSA and the Haute autorité pour la diffusion des oeuvres et la protection des droits sur internet (Hadopi). Arcom allocates broadcasting licences and

is tasked with the implementation of online space regulations. It is also the national authority charged with facilitating the implementation of the Digital Services Act (DSA) in France.

The adaptation of the French counterdisinformation assemblage to Covid and the strategic disinformation campaigns led to attempts at a strong regulation of the platforms and (more successfully) an institutional development of the governmental core of the assemblage. The securitisation of the disinformation weakening the epistemic foundations of the state, which was already present as a result of Russia's electoral interference, and, moreover, could build on the earlier securitisation of radical Islamist movements' communication campaigns, intensified. In spite of its interest in claiming sovereignty over the national informational domain, the government's political technology of choice was regulation and institutional capacity development rather than direct prohibitionist and punitive ("sovereign") interventions to counter threats of "digital interference" (*ingérences numériques*) by foreign powers. The French counterdisinformation assemblage developed a strong institutional core focused on early threat identification and response, understood in terms of both strategic communications and active measures (*ripistes*). The Operational Committee for the Combat Against Information Manipulations (COLMI), chaired by the SGDSN; Viginum, the intelligence services and the foreign, defence and interior ministries were all key bodies involved in the performance of the former task. The foreign and defence ministries were also particularly active in performing the second task. However, since its inception, the assemblage has also manifested a certain distributive quality with a dense network of, e.g., fact checking entities that are either NGOs or affiliates of the established media; as well as media literacy initiatives such as *Entre les lignes*, which expanded during Covid with the aim to increase societal resilience against the dissemination of disinformation. Last but not least, ever since its inception, the French counterdisinformation policy was designed to actively shape and make use of the EU's efforts.

THE CZECH REPUBLIC

The Czech counterdisinformation assemblage gradually formed in the aftermath of Russia's first aggression against Ukraine in 2014 (for a detailed overview see (EBERLE & DANIEL, 2023)). During the second half of that year, and especially in 2015–2016, the issue of pro-Russian disinformation

was first picked up by journalists from leading liberal media (*Respekt*, *Hospodářské noviny*). In this, they were joined by civil society actors – think-tanks and NGOs like European Values, the Prague Security Studies Institute, Jagello 2000 or, later, the Czech Elves. These actors started assembling lists of disinformation websites, publishing op-eds, organising seminars, and launching fact-checking initiatives and media literacy programmes. Non-state actors were – and still are – key to the counter-disinformation assemblage in Czechia (for an overview see (SYROVÁTKA, 2021)), with new initiatives appearing (and disappearing) every year.

In contrast, the involvement of state actors has ebbed and waned, depending on the changing levels of political support for the counter-disinformation agenda, among other things. From the very beginning, security institutions were closely engaged in the assemblage, especially the domestic counterintelligence Security Information Service (BIS) and a newly created unit at the Ministry of the Interior – the Centre against Terrorism and Hybrid Threats (CTHH). However, they enjoyed varying levels of political support from the Sobotka (2013–2017) and Babiš (2017–2021) governments, as well as different degrees of involvement of other state actors, such as the armed forces. The close involvement of security institutions meant that the question of disinformation was predominantly approached through a security lens, and disinformation was often presented as a part of a broader coordinated campaign of ‘information war’ or ‘hybrid warfare’. This was visible in official documents, especially the *National Security Audit* (Ministry of the Interior of the Czech Republic 2016), but also the *Defence Strategy* (MINISTRY OF DEFENCE OF THE CZECH REPUBLIC, 2017), which explicitly labelled “targeted disinformation activities” as part of Russia’s “hybrid campaign” (IBID., P. 7). Some contestation of the securitising logic – even if it was rather partial, implicit and reluctant – came from NGOs and academics approaching the problem of disinformation as a matter of critical thinking and media literacy (GREGOR & VEJVODOVÁ, 2018; NUTIL, 2018). From the beginning, social media were considered as an important site for disinformation production and dissemination, and of countering it. They were seen as a channel through which the external enemy – especially Russia – was able to penetrate and corrupt the social body through “their manipulative use, disinformation campaigns and propaganda” (MINISTRY OF THE INTERIOR OF THE CZECH REPUBLIC, 2016, P. 128). Monitoring of social media, especially Facebook groups, then became a key activity of prominent civil society actors, such as the Czech Elves.

The response by the Czech counterdisinformation assemblage to Covid could then be separated into two parallel tracks. The first was that of the government, which lacked a coherent strategy to respond to the pandemic itself, and came with only very limited initiatives in regard to countering the related disinformation. The second was the civil society response, which was spontaneous and rather extensive, often making up for the missing role of the state. On the one hand, these nonstate actors participated in securitising Russia and China, as well as promoting the official vaccination line to the public. On the other hand, these efforts proved socially divisive.

The communication by the government was hyperpersonalised, with Prime Minister Andrej Babiš presenting himself as a bold leader who is simultaneously courageous, responsive to the demands of the people and “one of us” – a prototypical Czech citizen (ZÁHRADNÍČKOVÁ & ŠEREK, 2023). From the very start, the government’s communication securitised the pandemic, amply using war rhetoric, mentioning battles against the virus, speaking about frontlines, etc. The reaction was compounded by the intergovernmental rivalries: various ministers sometimes argued with each other on social platforms and competed for purchases of medical equipment from other countries. This style of communication “created something which can be called permanent chaos” (EIBL & GREGOR, 2021, P. 267). Some of the institutions tasked with countering disinformation, such as the Centre against Terrorism and Hybrid Threats (CTHH), indeed played their part, e.g. by compiling and publicising a list of Covid-related disinformation (CENTRUM PROTI TERORISMU A HYBRIDNÍM HROZBÁM, UNDATED) – thus mirroring EEAS’s activity on the national level. But the effectiveness of their efforts was limited by the inept communication of the government as a whole.

The failures of the government led to an intense reaction from civil society. A number of do-it-yourself activities started to be organised soon after the pandemic outbreak, especially to counter the problem of the lack of masks. Groups and individuals shared their experiences in online fora while new apps (such as eRouška) were also developed without the government’s support to navigate people through the pandemic (CHARVÁT, 2021). There were also a number of specifically counterdisinformation activities by both established non-state actors and newcomers. Among the former were the *Vaccine against Disinformation* by the NGO European Values (EUROPEAN VALUES, 2020) and *Disinformation Disinfection by People in*

Need (DEZINFORMAČNÍ DEZINFEKCE, UNDATED). Among the latter was the collective *C19 Disinfoservice*, a cooperation of a leading news website, *Seznam Zprávy*, with technological companies, academics and NGOs (SEZNAM ZPRÁVY, UNDATED). These initiatives focused on monitoring and debunking Covid-related disinformation that was being circulated on social media, and via 'alternative' websites as well as chain mails.

Overall, the Covid pandemic helped to both solidify the core of the counterdisinformation assemblage, and spur its further growth, which led to a certain diversification. Due to the mainstreaming of the counterdisinformation agenda during Covid, the key actors of the assemblage, that is, those who already possessed expertise and resources, could rather easily use the opportunity and increase their exposure in both traditional and social media channels. The solidification of the assemblage core was reflected in the increased public role of nonstate actors such as the Czech Elves or the Semantic Vision company, whose outputs and commentaries became highly visible in the media. On the state side, the government, after some hesitation, finally adopted its *National Strategy for Countering Hybrid Interference* (MINISTRY OF DEFENCE, 2021) and supported it with a social media campaign. The strategy was not explicitly tied to the Covid context save some public statements (ČESKÝ ROZHLAS, 2020), instead setting broader objectives of state, societal and critical infrastructure resilience. It also shied away from naming specific external hostile actors. The aggravated level of the threat of disinformation campaigns during Covid, however, facilitated keeping the issue high on the security agenda and resulted in a comparatively unique and ambitious document. On the parliamentary level, a special Permanent Commission was set up (LANGŠÁDLOVÁ, 2020) with a leading role for opposition politicians, who would now push the issue – and continue doing so in prominent roles under the Fiala government, which was in office in 2021–2025.

In this core of the assemblage, the drive towards securitisation of disinformation continued and was even reinforced by the increasing tensions with both Russia and China. These tensions resulted from a series of diplomatic frictions and incidents, from the controversial visit of the President of the Czech Senate to Taiwan (ZELENKA, 2021A, 2021B) to the April 2021 revelation that the until then unexplained 2014 explosions in a Czech ammunition depot near the village of Vrbětice – which killed two people – were in fact the work of Russian intelligence operatives. In this

logic, Covid disinformation was approached primarily as yet another tool of Russian and Chinese influence activities. This also solidified the role of the *Security Intelligence Service* (BIS) as a key actor, as it now engaged in an ever more proactive communication with the public (DITRYCH, 2020). On the other hand, the unprecedented scope of the Covid disinformation led also to the rise of a set of actors with a parallel and rather distinct perspective in which disinformation is seen primarily as a social issue (EBERLE & DANIEL, 2023). This led to the rise of a parallel (and much less influential) group within the counterdisinformation assemblage, which focused mostly on researching the spread and effects of disinformation in the Czech public (STEM, 2021).

CONCLUSION: A STAYING CONFRONTATION

The Covid pandemic outbreak created a global health crisis as well as a fertile ground for strategic disinformation campaigns in liberal societies that targeted their epistemic foundations. Hand in hand with the securitisation of the evolving disinformation assemblages under the broad rubric of hybrid threats, the counterdisinformation assemblage as a multilevel composite of security rationalities, technologies and practices to counter the threat, developed to restabilise the EU's internal political space. This counterdisinformation assemblage provided an overall strategic direction to the efforts to counter the epistemological challenge to the member states posed by strategic disinformation campaigns deployed as a means of statecraft in the conditions of rising geopolitical contestation. However, elements of this assemblage evolved in tactically different, sometimes nonlinear ways, acting on each other across different levels. The cases of France and the Czech Republic show how even in the conditions of a successful securitisation of strategic disinformation, the constitution of the countersecurity apparatuses could take different pathways, as it could reflect and adapt to specific political and cultural contexts – for example, the strong desire to enact digital sovereignty in the French case and the legal obstacles to it, and the more socially diffused operation of the apparatus in the Czech case yet with curious tendencies toward a discursive militarisation nonetheless – as well as interests of governmental and nongovernmental actors (sometimes mutable over time) pertaining to which disinformation narratives and discursive frames would be targeted by security practices or who would be included in the counterdisinformation assemblage and who would not.

The legacies of the innovation and adaptation of both the disinformation and counterdisinformation assemblages during the pandemic remain relevant in the ongoing contestation over the epistemic foundations of the EU member states today against the background of a wider (geo-)political contestation in global politics. Strategic propaganda *forming* alternative realities and strategic disinformation campaigns aiming at *subverting* hegemonic regimes of truth will continue to aim to manipulate political outcomes in liberal democracies through electoral interference provided that elections will remain central as decision points in liberal politics. However, as foreshadowed during the adaptation of the disinformation assemblages during Covid, these campaigns increasingly focus also on undermining the epistemic foundations of liberal political orders, with an ongoing shift toward the cognitive domain concerning the shared notion of truthful representation – that is, there is a shift from the focus on the uptake of intentionally misleading information toward an information processing through manipulation of a *priori* established interpretive frames, filters, emotions and heuristics (CATENA, DITRYCH & KOVALČÍKOVÁ, 2025). Shared notions of truth about what is will remain a subject of contestation in which the disruption function enacted by disinformation assemblages, and the maintenance or restoration by the counterdisinformation assemblages related to the interiorisation function of the state will seek to outcompete each other. The assemblage theory, positing these assemblages as foundationless yet strategic, complementary, emergent and productive of social relations and power, can contribute to reinvigorating the critical research on disinformation and propaganda. In so doing, it can help us to grasp the broader challenge of truth contestation being weaponised as an important dimension of the great power conflict.

ENDNOTES

- 1 In the EEAS's words, "the work of independent media and fact checkers is crucial to deliver[ing] reliable and authoritative information about the pandemic" and "paramount in mitigating the potential harmful consequences and enhancing societal resilience." *EEAS Special Report Update: Short Assessment of Narratives and Disinformation around the Covid 19 Pandemic*, 20 May and 2 Dec. 2020.
- 2 "Empowering citizens to critically analyse information online is key to addressing disinformation." *Tackling the Covid-19 Disinformation*, op. cit.
- 3 Two days before the second round of the presidential election, in which Emmanuel Macron competed with Marine Le Pen, ca. 20,000 emails from the Macron campaign, to which a few forged ones with scandalous content were added, were made public on a *4Chan* forum to be quickly spread further by pro-Kremlin social media accounts (see Hénin, 2023).
- 4 Before the law entered into force, the Constitutional Council ruled that the judge (*juge des référés*) could order a removal of information only if it was evidently false or misleading, and also if there was a clear risk that it could impact on the vote.
- 5 "Russia Today et Sputnik ne se sont pas comportés comme des organes de presse et des journalistes, mais ils se sont comportés comme des organes d'influence, de propagande, et de propagande mensongère, ni plus, ni moins [Russia Today and Sputnik did not behave like news outlets and journalists, but rather like instruments of influence, propaganda and disinformation – nothing more, nothing less]," President Macron stated during the press conference with Vladimir Putin in Versailles on May 29, 2017. Cf. *France Info* (29 May 2017).
- 6 *Portal Kombat* was a label given to a network of at least 193 portals disseminating content legitimising Russia's war on Ukraine while seeking to undermine Western societies' support for Ukraine's defence. Matrioshka specifically targeted fact-checking affiliates of major media such as BFMZV, Le Parisien, Libération, and Le Monde as well as Banque de France and DGSI, the French counterintelligence. See "Comment fonctionne Matriochka, la dernière campagne de désinformation pro-russe débusquée par la France," *Télérama* (11 June 2024), available at: <https://www.telerama.fr/debats-reportages/comment-fonctionne-matriochka-la-derniere-campagne-de-desinformation-pro-russe-debusquee-par-la-france-7020812.php>.
- 7 According to the official decree it was mandated to engage in "computerised and automated processing of personal data... to detect and describe operations that directly or indirectly involve a foreign state or a foreign nonstate entity [and] that are aimed at the artificial or automated, mass and deliberate dissemination [...] of allegations or imputations of facts that are manifestly inaccurate or misleading and are likely to harm the fundamental interests of the state." Décret No. 2021-1587 (7 December 2021), available at: <https://www.legifrance.gouv.fr/eli/decret/2021/12/7/PRMD2131887D/jo/texte>.

REFERENCES

- A Abrahamsen, R., & Williams, M.C. (2009). Security beyond the state: Global security assemblages in international politics. *International Political Sociology*, 3(1), 1–17. <https://doi.org/10.1111/j.1749-5687.2008.00060.x>
- Acuto, M., & Curtis, S. (2014). Reassembling international theory: Assemblage thinking and international relations. *International Political Sociology*, 8(3), 341–356. <https://doi.org/10.1057/9781137383969>
- Adler, E., & Drieschova, A. (2021). The epistemological challenge of truth subversion to the liberal international order. *International Organisation*, 75(2), 359–386. <https://doi.org/10.1017/S0020818320000533>
- Agajanian, T., & Moran, R.E. (2025). Gender as a central site of inquiry within mis- and disinformation studies. *Feminist Media Studies*, 25(7), 1739–1743. <https://doi.org/10.1080/14680777.2024.2332643>
- Aradau, C. (2017). Assembling (non)knowledge: Security, law and surveillance in a

- digital world. *International Political Sociology*, 11(4), 327–342. <https://doi.org/10.1093/ips/olx019>
- Assemblée Nationale (2018). *Proposition de loi relative à la lutte contre la minuplation de l'information*. https://www.assemblee-nationale.fr/dyn/15/textes/115t0190_texte-adopte-provisoire.pdf
- Aytac, U. (2024). Digital domination: Social media and contestatory democracy. *Political Studies*, 72(1), 6–25. <https://doi.org/10.1177/00323217221096564>
- Azzimonti, M., & Fernandes, M. (2023). Social media networks, fake news, and polarisation. *European Journal of Political Economy*, 76. <https://doi.org/10.1016/j.ejpoleco.2022.102256>
- B
Badouard, R. (2020). La régulation des contenus sur Internet à l'heure des "fake news" et des discours de haine. *Communications*, 106(1), 161–173. <https://doi.org/10.3917/commu.106.0161>
- Bak, P. D. P., Walter, J. G., & Bechmann, A. (2023). Digital false information at scale in the European Union: Current state of research in various disciplines, and future directions. *New Media & Society*, 25(10), 2800–2819. <https://doi.org/10.1177/1461444822112214>
- Bastick, Z. (2021). Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation. *Computers in Human Behavior*, 116 (March), 106633. <https://doi.org/10.1016/j.chb.2020.106633>
- Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. *Alternatives*, 27(1). <https://doi.org/10.1177/03043754020270S10>
- 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. *Journal of Common Market Studies*, 62(5), 1395–1407. <https://doi.org/10.1111/jcms.13548>
- Bradshaw, S., & DeNardis, L. (2022). *Internet infrastructure as an emerging terrain of disinformation*. Waterloo (CAN): Centre for International Governance Innovation.
- Brambilla, C. (2015). Exploring the critical potential of the borderscapes concept. *Geopolitics*, 20(1), 14–34. <https://doi.org/10.1080/14650045.2014.884561>
- Bueger, C. (2017). Territory, authority, expertise: Global governance and the counter-piracy Assemblage. *International Political Sociology*, 11(2), 163–181. <https://doi.org/10.1177/1354066117725>
- Bušťíková, L., & Baboš, P. (2020). Best in Covid: Populists in the time of pandemic. *Politics and Governance*, 8(4), 496–508. <https://doi.org/10.17645/pag.v8i4.3424>
- Butler, J. (2004). *Precarious life: The powers of mourning and violence*. London–New York: Verso.
- C
Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: The case of EU cybersecurity policy. *Journal of European Integration*, 42(8), 1111–1126. <https://doi.org/10.1080/07036337.2020.1853122>
- 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(1), 1–10. <https://doi.org/10.1057/s41599-023-02179-8>
- Catena, B., Ditrych, O., & Kovalčíková, N. (2025). *Smoke and mirrors: Building EU resilience against manipulation through cognitive security*. Paris: European Union Institute for Security Studies.
- Centrum proti terorismu a hybridním hrozbám [The Centre Against Terrorism and Hybrid Threats]. *Koronavirus: Přehled hlavních dezinformačních sdělení [Coronavirus: An overview of the main disinformation naratives]* (undated). <https://www.mvcr.cz/chh/clanek/koronavirus-prehled-hlavnich-dezinformacnich-sdeleni.aspx>
- Český rozhlas. (2020, November 13). Náměstek Havránek: Vytvoření strategie pro boj s hybridními hrozbami je teď hlavní prioritou [Deputy Minister Havránek: Creating a strategy to combat hybrid threats is now the main priority]. *Český rozhlas*. https://www.irozhlas.cz/zpravy-domov/jan-havranek-boj-s-hybridnimi-hrozbami_2011131532_ada

- Charon, P., & Jeangène Vilmer, J.-B. (2021). *Chinese Influence Operations. A Machiavellian Mome*. Paris: IRSEM.
- Charvát, O. (2021, March 6). Česko selhává v digitalizaci a otevřeném sdílení dat. Stát nahrazuje občanská společnost [The Czech Republic is failing in digitalisation and open data sharing: Civil society is replacing the state]. *Hospodářské noviny*. <https://domaci.hn.cz/cl-66891880-cesko-selhava-v-digitalizaci-a-otevrenem-sdileni-dat-stat-nahrazuje-obcanska-spolecnost>
- Cohen, C. (2021, October 15). Viginum, l'arme de l'État contre les ingérences numériques étrangères, lancée ce vendredi. *Le Figaro*. <https://www.lefigaro.fr/medias/viginum-l-arme-de-l-etat-contre-les-ingerences-numeriques-etrangeres-sur-le-pied-de-guerre-avant-la-presidentielle-201921>
- Conrad, M. (2022). A post-truth campaign? The alternative for Germany in the 2019 European parliament elections. *German Politics and Society*, 40(1), 58–76. <https://doi.org/10.3167/gps.2022.400104>
- Conrad, M., & Newman, S. (2024). Conclusions: 'Mainstream' alarmism or 'critical' complacency? How to approach post-truth populism. In S. Newman, & M. Conrad (Eds.), *Post-truth populism* (pp. 333–342). Lon-don: Palgrave Macmillan.
- Cosentino, G. (2020). The post-truth world order. In G. Cosentino, *Social media and the post-truth world order: The global dynamics of disinformation* (pp. 1–32). Palgrave Pivot Cham.
- Council of the European Union. (undated). Disinformation and democratic resilience. <https://www.consilium.europa.eu/en/policies/disinformation-and-democratic-resilience/>
- Czerniak, K., Pillai, R., Parmar, A., Ramnath, K., Krocke, J., & Myneni, S. (2023). A scoping review of digital health interventions for combating COVID-19 misinformation and disinformation. *Journal of the American Medical Informatics Association*, 30(4), 752–760. <https://doi.org/10.1093/jamia/ocad005>
- D De Landa, M. (2006). *A new philosophy of society: Assemblage theory and social complexity*. London: Bloomsbury.
- Deleuze, G. (1992). What is a dispositif? In T. Armstrong (Ed.), *Michel Foucault: philosopher*. Harvester Wheatsheaf.
- Deleuze, G., & Guattari, F. (1987). *A thousand plateaus: Capitalism and schizophrenia*. University of Minnesota Press.
- Della Lena, S. (2024). The spread of misinformation in networks with individual and social learning. *European Economic Review*, 168. <https://doi.org/10.1016/j.eurocorev.2024.104804>
- Dezinformační dezinfekce (undated). *Dezinformační dezinfekce – výukové materiály ke (koronavirovým) dezinformacím*. People in Need. <https://www.jsns.cz/projekty/medialni-vzdelavani/materialy/publikace/dezinformacni-dezinfekce>
- Ditrych, O. (2020). 'Who let the dogs out': The Czech Intelligence Service Annual Report and the challenges of discussing threats in a postfactual age. *RUSI Commentary*.
- Ditrych, O. (2026). Navigating and shaping the foreign information manipulation landscapes. In M. Conrad, & S. Newman (Eds.), *Reclaiming liberal democracy in the postfactual age*. De Gruyter.
- Dittmer, J. (2013). Geopolitical assemblages and complexity. *Progress in Human Geography*, 38(3). <https://doi.org/10.1177/0309132513501405>
- Dittmer, J. (2017). *Diplomatic material*. Duke University Press.
- Doucet, M. (2016). Global assemblages of security governance and contemporary international intervention. *Journal of Intervention and Statebuilding*, 10(1), 116–132. <https://doi.org/10.1080/17502977.2015.1054656>
- E Eberle, J., & Daniel, J. (2022). Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety. *Political Geography*, 92. <https://doi.org/10.1016/j.polgeo.2021.102502>

Eberle, J., & Daniel, J. (2023). *Politics of hybrid warfare: The remaking of security in Czechia after 2014*. Palgrave Macmillan.

EEAS. (2015). *The European Union in a changing global environment: A more connected, contested and complex world*. EEAS.

EEAS. (2020a, May 20). *EEAS special report update: Short assessment of narratives and disinformation around the Covid 19 pandemic*.

EEAS. (2020b, April 1). *EEAS special report update: Short assessment of narratives and disinformation around the Covid 19 pandemic*.

EEAS. (2020c, March 19). *EEAS special report update: Short assessment of narratives and disinformation around the Covid 19 pandemic*.

EEAS. (2020d, April 24). *EEAS special report update: Short assessment of narratives and disinformation around the Covid 19 pandemic*.

EEAS. (2020e, December 2). *EEAS special report update: Short assessment of narratives and disinformation around the Covid 19 pandemic*.

Eibl, O., & Gregor, M. (2021). The Czech Republic: Self-proclaimed role models. In D. Lilleker, I. A. Coman, M. Gregor, & E. Novelli (Eds.), *Political communication and COVID-19* (pp. 259–268). Routledge.

Ekman, A., & Everts, S. (2024). *Contestation: The new dynamic driving global politics*. European Union Institute of Security Studies.

Elbe, S. (2022). Who owns a deadly virus? Viral sovereignty, global health emergencies, and the matrix of the international. *International Political Sociology*, 16(2). <https://doi.org/10.1093/ips/olab037>

Elbe, S., Vorlíček, D., & Brenner, D. (2023). Rebels, vigilantes and mavericks: Heterodox actors in global health governance. *European Journal of International Relations*, 29(4), 903–928. <https://doi.org/10.1093/ips/olab037>

European Commission. (2022). *The strengthened code of practice on disinformation*. <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>

European Commission. (2025). *European Democracy Shield: Empowering strong and resilient democracies*. JOIN(2025) 791 final.

European Council. (2022, March 2). *Press release* (2 Mar. 2022) citing HR/VP Josep Borrell.

European Democracy Action Plan. (2020). *European Democracy Action Plan*, COM(2020) 790.

European Security Union Strategy. (2020, December 15). *EU Security Union Strategy*, COM(2020) 605 FI-NAL; Council Conclusions on Strengthening Resilience and Countering Hybrid Threats, including Disinformation in the Context of the COVID-19 Pandemic.

European Values (2020, December 8). *Bezpečnostní centrum Evropské hodnoty spouští informační kampaň Vakcína proti dezinformacím* [European Values Security Centre launches the information campaign Vaccine Against Disinformation]. European Values. <https://europeanvalues.cz/cs/press-release-european-values-center-for-security-policy-launches-information-campaign-vaccine-against-disinformation/>

F

Fauroux, V. (2024, March 7). *ENQUÊTE – Désinformation: comment la Russie mène une guerre secrète en France*. *Tf1*. <https://www.tf1info.fr/international/video-guerre-ukraine-russie-enquete-desinformation-comment-la-russie-mene-une-guerre-secrete-en-france-2288659.html>

Florentino, M.-R. (2018, November 22). *France passes controversial fake news law*. *Euronews*. <https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law>

Foucault, M. (2000). Truth and power. In J. Faubion, J. (Ed.), *The essential works of Foucault* (Vol. 3). New Press.

- G Gallotti, R., Valle, F., Castaldo, N., Sacco, P., & De Domenico, M. (2020). Assessing the risks of “infodemics” in response to COVID-19 epidemics. *Nature Human Behaviour*, 4(12), 1285–1293. <https://doi.org/10.1038/s41562-020-00994-6>
- Gregor, M., & Vejvodová, J. (2018). *Nejlepší kniha o fake news!!! [The best book about fake news!!!]*. Cpress.
- Guibert, N., & Pedroletti, B. (2021, September 3). Infektion 2.0, l'opération chinoise d'inspiration russe censée faire oublier l'origine du Covid-19. *Le Monde*. https://www.lemonde.fr/international/article/2021/09/03/infektion-2-0-l-operation-chinoise-d-inspiration-russe-destinee-a-faire-oublier-l-origine-du-covid-19_6093241_3210.html
- Guillaume, M. (2019). *Combating the manipulation of information: A French case*. Hybrid Centre of Excellence.
- H Hameleers, M. (2024). The nature of visual disinformation online: A qualitative content analysis of alternative and social media in the Netherlands. *Political Communication*, 42(1), 108–126.
- Harrison, R. (2021). Tackling disinformation in times of crisis: The European Commission's response to the Covid-19 infodemic and the feasibility of a consumer-centric solution. *Utrecht Law Review*, 17(3), 18–33. <https://doi.org/10.36633/ulr.675>
- Hayward, T. (2025). The problem of disinformation: A critical approach. *Social Epistemology*, 39(1), 1–23. <https://doi.org/10.1080/02691728.2024.2346127>
- Heiss, R., Waser, M., Falkenbach, M., & Eberl, J. M. (2021). *How have governments and public health agencies responded to misinformation during the COVID-19 pandemic in Europe*. European Observatory on Health Systems and Policies.
- Helm, R. K., & Nasu, H. (2021). Regulatory responses to ‘fake news’ and freedom of expression: Normative and empirical evaluation. *Human Rights Law Review*, 21(2), 302–328. <https://doi.org/10.1093/hrlr/ngaa060>
- Hénin, N. (2023). *Disinformation landscape in France*. EU Disinfo Lab. <https://www.disinfo.eu/publications/disinformation-landscape-in-france/>
- Hoboken, J., & Ó Fathaigh, R. (2021). Regulating disinformation in Europe: Implications for speech and privacy. *UC Irvine Journal of International, Transnational, and Comparative Law*, 6(1), 9–36.
- I Iskandrova, T. (2024). *Unveiling semiotic codes of fake news and misinformation*. Macmillan.
- J Joint Communication. (2016). *Joint communication to the European Parliament and the Council: Joint framework on countering hybrid threats, a European Union response*, JOIN/2016/018 FINAL.
- Joint Communication. (2018). *Joint communication to the European Parliament, the European Council and the Council: Increasing resilience and bolstering capabilities to address hybrid threats*, JOIN(2018) 16 FINAL.
- Jones, M., Jones, R., & Woods, M. (2004). *An introduction to political geography: Space, place and politics*. Routledge.
- K Kachelmann, M., & Reiners, W. (2023). The European Union's governance approach to tackling disinformation—protection of democracy, foreign influence, and the quest for digital sovereignty. *L'Europe en Formation*, 396(1), 11–36. <https://doi.org/10.3917/e.eufor.396.0011>
- L Langšádlová, H. (2020, June 26). *Langšádlová: Zahraniční investice mohou být pro Česko hrozbou, zejména ty čínské [Langšádlová: Foreign investments could threaten the Czech Republic – especially those from China]*. TOP09.
- Lim, G., & Bradshaw, S. (2023). *Chilling legislation: Tracking the impact of ‘fake news’ laws on press freedom internationally*. Center for International Media Assistance.
- López-Lucia, E., & de Almagro, M. (2023). Introduction: Transnational assemblages and the production of security knowledges. *Territory, Politics, Governance*, 12(4). <https://doi.org/10.1080/21622671.2023.2271524>
- M Malhotra, P., Hall, N.-A., Xia, Y., Stahl, L., Chadwick, A., Vaccari, A., & Lawson, B. (2025). *Unpacking credibility evaluation on digital media: A case for interpretive qualitative approaches*.

- Annals of the International Communication Association (online first). <https://doi.org/10.1093/anncom/wlaf008>
- Marcus, G., & Saka, E. (2006). Assemblage. *Theory, Society & Culture*, 23(2–3), 101–106. <https://doi.org/10.1177/0263276406006257>
- Mathevon, F. (2021, October 15). Viginum, l'agence gouvernementale qui lutte contre les ingérences numériques étrangères entre en piste. *Radio France*. <https://www.radiofrance.fr/franceinter/viginum-l-agence-gouvernementale-qui-lutte-contre-les-ingérences-numeriques-etrangeres-entre-en-piste-1780820>
- McFarlane, C. (2009). Translocal assemblages: Learning, space and development. *Geoforum*, 40(4), 561–567. <https://doi.org/10.1016/j.geoforum.2009.05.003>
- Ministry of Defence of the Czech Republic. (2017). *Defence strategy*. <https://www.mo.gov.cz/assets/en/ministry-of-defence/strategy-and-doctrine/defencestrategy2017.pdf>
- Ministry of Defence of the Czech Republic. (2021). *National strategy for countering hybrid interference*. <https://www.mo.gov.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf>
- Ministry of the Interior of the Czech Republic. (2016). *National security audit*. <https://mv.gov.cz/chh/clanek/audit-narodni-bezpecnosti.aspx>
- Monsees, L. (2023). Information disorder, fake news and the future of democracy. *Globalizations*, 20(1), 153–168.
- Müller, M. (2015). Assemblages and actor-networks: Rethinking socio-material power, politics and space. *Geography Compass*, 9(1), 27–41. <https://doi.org/10.1111/gec3.12192>
- N Nutil, P. (2018). *Média, lži a příliš rychlý mozek – Průvodce postpravdivým světem [Media, lies, and an overly fast brain: A guide to the post-truth world]*. Praha: Grada.
- O Ong, A., & Collier, S.J. (Eds.). (2005). *Global assemblages: Technology, politics, and ethics as anthropological problems*. Blackwell Publishing.
- P Pasquetto, I., Lim, G., & Bradshaw, S. (2024). Misinformed about misinformation. *Harvard Kennedy School Misinformation Review*, 5(5). <https://doi.org/10.37016/mr-2020-159>
- Pasquetto, I., Olivieri, A., Tacchetti, L., Riotta, G., & Spada, A. (2022). Disinformation as infrastructure: Making and maintaining the QAnon conspiracy on Italian digital media. *Proceedings of the ACM on Human-Computer Interaction*, 6, 1–31. <https://doi.org/10.1145/3512931>
- Peukert, A. (2024). The regulation of disinformation: A critical appraisal. *Journal of Media Law*, 16(1), 1–7. <https://doi.org/10.1080/17577632.2024.2362485>
- Polletta, F., & Callahan, J. (2017). Deep stories, nostalgia narratives, and fake news: Storytelling in the Trump era. *American Journal of Cultural Sociology*, 5(3), 392–408. <https://doi.org/10.1057/s41290-017-0037-7>
- R Radu, R. (2020). Fighting the 'infodemic': Legal responses to COVID-19 disinformation. *Social Media + Society*, 6(3). <https://doi.org/10.1177/205630512094819>
- Rajaram, P.K., & Grundy-Warr, C. (Eds.). (2007). *Borderscapes: Hidden geographies and politics at territory's edge*. University of Minnesota Press.
- Rød, B., Pursiainen, C., & Eklund, N. (2025). Combatting disinformation – How do we create resilient societies? Literature review and analytical framework. *European Journal for Security Research*, 10, 73–114. <https://doi.org/10.1007/s41125-025-00105-4>
- Rychnovská, D. (2021). Rethinking the infodemic: Global health security and distributed accountability in Europe. *Czech Journal of International Relations*, 56(4), 77–90. <https://doi.org/10.32422/mv-cjir.1817>
- S Sassen, S. (2006). *Territory, authority, rights: From medieval to global assemblages*. Princeton University Press.
- Saurwein, F., & Spencer-Smith, C. (2020). Combating disinformation on social media: Multilevel governance and distributed accountability in Europe. *Digital Journalism*, 8(6): 820–841. <https://doi.org/10.1080/21670811.2020.1765401>

- Sénat. (2020, April). *Désinformation, cyberattaques, cybermalveillance: l'autre guerre du Covid 19*, DLC No. 125. https://www.senat.fr/fileadmin/import/files/fileadmin/Fichiers/Images/commission/affaires_etrangeres/Coronavirus_suivi/4_pages_-_CYBER_vedf160420-2_01.pdf
- Seznam zprávy (Undated). Iniciativa C19 Dezinfoservis. *Seznam Zprávy*. <https://www.seznamzpravy.cz/autor/iniciativa-c19-dezinfoservis-772>
- Simion, M. (2024). Knowledge and disinformation. *Episteme*, 21(4), 1208–1219, <https://doi.org/10.1017/epi.2023.25>
- Sky News. (2021, August 11). Covid 19: Firm that claimed Pfizer vaccine turns people into chimpanzees banned from Facebook. https://news.sky.com/story/covid-19-network-of-accounts-that-claimed-vaccine-turns-people-into-chimps-taken-down-by-facebook-12378533?utm_source=chatgpt.com
- Smith, S., Kao, E., Mackin, E., Shah, D., Simek, O., & Rubin, D. (2021). Automatic detection of influential actors in disinformation networks. *PNAS*, 118(4), <https://doi.org/10.1073/pnas.2011216118>
- Sociétés civiles. (2018, May 4). *Sociétés civiles, médias et pouvoirs publics: les démocraties face aux manipulations de l'information*. The Conference on Manipulation of Information, Paris, France.
- Starbird, K. (2019). Disinformation's spread: Bots, trolls and all of us. *Nature*, 571, 7766. <https://doi.org/10.1038/d41586-019-02235-x>
- Starbird, K., Arif, A., & Wilson, T. (2019). Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations. *Proceedings of the ACM on Human-Computer Interaction*, 3, 1–26. <https://doi.org/10.1145/335922>
- STEM (2021, April 16). *Studie: Covid-19 a šířitelé konspiračních teorií [Study: COVID-19 and disseminators of conspiracy theories]*. STEM. <https://www.stem.cz/studie-covid-19-a-siritele-konspiracnich-teorii/>
- Storeng, K. T., & De Bengy Puyvallée, A. (2021). The smartphone pandemic: How Big Tech and public health authorities partner in the digital response to Covid-19. *Global Public Health*, 16(8–9), 1482–1498. <https://doi.org/10.1080/17441692.2021.1882530>
- Syrovátka, J. (2021). Civil society initiatives tackling disinformation: Experiences of Central European countries. In M. Gregor, & P. Mlejnková (Eds.), *Challenging online propaganda and disinformation in the 21st century* (pp. 225–253). Springer International Publishing.
- T Tackling the Covid-19. (2020). *Tackling the Covid-19 Disinformation: Getting the Facts Right*, JOIN(2020) 8 FINAL.
- Tandoc Jr, E. C., Lim, Z. W., & Ling, R. (2017). Defining “fake news” A typology of scholarly definitions. *Digital journalism*, 6(2), 137–153. <https://doi.org/10.1080/21670811.2017.1360143>
- Tripodi, F., Garcia L., & Marwick, A. (2024). ‘Do your own research’: Affordance activation and disinformation spread. *Information, Communication & Society*, 27(6). <https://doi.org/10.1080/1369118X.2023.2245869>
- U Urakami, J., Oura, H., Kim, Y., & Seaborn, K. (2022). Finding strategies against misinformation in social media: A qualitative study. *arXiv*. <https://arxiv.org/pdf/2205.00188>
- V Valaskivi, K., & Robertson, D. G. (2022). Introduction: Epistemic contestations in the hybrid media environment. *Popular Communication*, 20(3), 153–161. <https://doi.org/10.1080/15405702.2022.2057998>
- Vérité, S. L. (2025). The collective securitization of ‘disinformation’ and the EU’s ban on Russia Today and Sputnik. *International Affairs*, 101(5), 1853–1876. <https://doi.org/10.1093/ia/iiaf139>
- Vérité, S. L., Bjola, C., & Koops, J. A. (2020). Tackling COVID-19 disinformation: Internal and external challenges for the European Union. *The Hague Journal of Diplomacy*, 15(4), 569–582. <https://doi.org/10.1163/1871191X-BJA10046>
- Vese, D. (2022). Governing fake news: The regulation of social media and the right to freedom of expression in the era of emergency. *European Journal of Risk Regulation*, 13(3),

477–513. <https://doi.org/10.1017/err.2021.48>

- W Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe Report No. 27. <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html>
- Z Zahradníčková, K., & Šerek, J. (2023). How populists construct public selves during the COVID-19 pandemic: A case study of the Czech prime minister. *Journal of Constructivist Psychology*, 36(1), 62–87. <https://doi.org/10.1080/10720537.2022.2082607>
- Zbieren, Randal. (2020). *Coronavirus et réseaux sociaux: Premières réflexions stratégiques sur une "info-démie"*. Fondation sur la recherche stratégique.
- Zelenka, J. (2021a, March 19). Hamáček využil čínské kontakty a sehnal roušky. Česko to stálo miliardy i „lokajské“ vítání na letišti [Hamáček used Chinese contacts to secure face masks. It cost the Czech Republic billions — and a “subservient” welcome at the airport]. *Deník N*. <https://denikn.cz/579636/hamacek-vyuzil-cinske-kontakty-a-sehnal-rousky-cesko-to-stalo-miliardy-i-lokajske-vitani-na-letisti/>
- Zelenka, J. (2021b). *Česko-čínské objímání* [The Czech-Chinese embrace]. N media.

NOTE

This manuscript was supported by the project “Reclaiming Liberal Democracy in Europe (RECLAIM)” within the Horizon Europe funding scheme. Website: <https://cordis.europa.eu/project/id/101061330>

AUTHOR BIOGRAPHY

Ondřej Ditrych leads the analysis of Russia and the Eastern Neighbourhood at the European Union Institute for Security Studies and lectures on global order and great powers at Sciences Po Paris. He previously served as Director of the Institute of International Relations Prague and Associate Professor of Political Science at Charles University. He writes on geopolitical risks, hybrid and cognitive threats, war and revolutionary violence. His most recent book, edited together with Jan Daniel and Jakub Zahora, is *Revolutionaries and Global Politics: War Machines from the Bolsheviks to ISIS*, published by Edinburgh University Press.

Jakub Eberle is Associate Research at the Institute for International Relations Prague. His professional interests involve theory of international relations, Czech and German foreign policy, politics of Central Europe, and critical approaches to digital politics.

Petr Kratochvíl is a full professor and a senior researcher at the Institute of International Relations in Prague, and a lecturer at the Metropolitan University Prague. His main research interests include the religion-politics nexus, critical geopolitics, and theories of international relations. He has published extensively on these topics, including in top journals such as *Geopolitics*, *Cooperation and Conflict*, *Politics and Religion*, and many others. His latest book is *Geopolitics of Global Catholicism: Politics of Religion in Space and Time*; his study titled “The Patriotic Turn in Russia: Political Convergence of the Russian Orthodox Church and the State?” (co written with Gaziza Shakhanova) received the 2023 Ted Jelen Award for the best article on religion and politics, awarded by the American Political Science Association.

Linda Monsees is a senior researcher at the Institute of International Relations Prague and Assistant Professor at Masaryk University Brno. Her research focuses on the politics of digital technology, digital sovereignty and the role of Big Tech in world politics. Her work has been published in *International Affairs*, *Globalizations* and *International Political Sociology*, among others.