Check for updates

Received: 10 April 2024 | Accepted: 31 July 2024

DOI: 10.1002/poi3.422

RESEARCH ARTICLE

P&I Policy & Internet PSO WILEY

Sanctions and infrastructural ideologies: Assessing the material shaping of EU digital sovereignty in response to the war in Ukraine

Niels ten Oever[1] | **Clement Perarnaud**[2] | **John Kristoff**[3] | **Moritz Müller**[4] | **Max Resing**[5] | **Arturo Filasto**[6] | **Chris Kanich**[3]

[1]Critical Infrastructure Lab, University of Amsterdam, Amsterdam, Netherlands

[2]Brussels School of Governance, Vrije Universiteit Brussel, Brussel, Belgium

[3]University of Illinois Chicago, Chicago, Illinois, USA

[4]SIDN Labs and University of Twente, Arnhem, Netherlands

[5]University of Twente, Enschede, Netherlands

[6]OONI, Rome, Italy

Correspondence

Niels ten Oever, Critical Infrastructure Lab, University of Amsterdam, Amsterdam, Netherlands.
Email: mail@nielstenoever.net

Funding information

Internet Society Foundation, Grant/Award Number: DB1/117723749.1; Ford Foundation, Grant/Award Numbers: A-202208-06454, 144895

Abstract

In this paper, we interrogate the sanctions instated against Russian media by the European Union (EU) in response to Russia's aggression in Ukraine. We do this in three ways. First, we present the outcome of extensive network measurements that show the heterogeneous implementation of the sanctions in EU Member States. Second, we explain how the sanctions fit the EU's digital sovereignty agenda. And third, we theorise the EU's digital sovereignty policies and sanctions as the emergence of a repressive state apparatus that forms a metagovernance regime with the ideological state apparatus of multistakeholder internet governance. We explain how networks are shaped in the dialectical relation between the ideological and repressive state apparatuses by showing how multistakeholder internet governance aims to stay politically neutral to accommodate the politics of different repressive state apparatuses. In turn, repressive state apparatuses define their demands in a technologically neutral way so multistakeholder internet governance can continue to develop and adapt communication networks. This research combines methods from Computer Science with theoretical frameworks from European Studies, Science and Technology Studies, Media Studies and International Relations. Through this work, we aim to contribute to the practice of interdisciplinary analysis of communication networks and debates on digital

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.
© 2024 The Author(s). *Policy & Internet* published by Wiley Periodicals LLC on behalf of Policy Studies Organization.

sovereignty, European infrastructuralisation, and internet governance.

KEYWORDS

digital sovereignty, EU, infrastructural ideologies, infrastructure, internet governance, sanctions, STS, Ukraine

INTRODUCTION

Sanctions are at the core of States' hard-power arsenal. Their imposition usually targets hostile State and non-State actors to deter or coerce them into new patterns of behaviour (Olsen, 2022). While economic sanctions have long impacted the technological sector, the Russian invasion of Ukraine led to unprecedented innovation on the EU level, with the adoption of a set of sanctions directly aimed at internet infrastructures.[1]

In 2022, the EU launched a series of sanction packages in response to the Russian invasion. Some of these packages' components were expressly dedicated to preventing the (online) broadcast of Russian state-backed media to EU territory. For the first time, EU operators received an order to ban the broadcast of specific media outlets funded by the Russian government (Poli & Finelli, 2023). The Council Decision 2022/351 stated in particular that "*it shall be prohibited for operators to broadcast or to enable, facilitate or otherwise contribute to broadcast, any content by the legal persons, entities or bodies listed in Annex XV, including through transmission or distribution by any means such as cable, satellite, IP-TV, Internet service providers, Internet video-sharing platforms or applications, whether new or pre-installed*" (The Council of the European Union, 2022).

This decision, followed by subsequent iterations, has been interpreted as a significant shift, departing from the traditional approach of the EU concerning media regulation and freedom. Indeed, it is "the first time that the Council has countered disinformation activities through restrictive measures" (Poli & Finelli, 2023), accounting for a significant evolution in the practice of sanctions.

Casero-Ripollés et al. (2023) qualify this turn as "unprecedented and controversial" and part of strengthening the EU's geopolitical approach towards disinformation. Helberger and Schulz (2022) argued further that before the start of the war, such a decision would have been considered "unthinkable" at the EU level, in light of its scope (covering both audiovisual and online media), its consequences for freedom of expression and access to information, but also because media regulation (as a cultural competency) had been mainly left to the responsibility of EU Member States until this point in time. Indeed, in normal circumstances, "the EU does not have the competence to impose on Member States restrictions on the activities of a broadcaster under media law" (Cabrera Blázquez, 2022).[2]

Similarly, as for cultural matters, the field of sanctions is known to give great preeminence to national governments at the EU level. Sanctions are formally adopted by the European Council and implemented independently by EU Member States. As we will see, sanction formulation has more recently been under the informal control of the Commission. It has become the tool enabling the Commission to give more substance to its geopolitical agenda (Portela, 2024).

The EU sanctions under study[3] are aimed at a series of Russian outlets, presented as a "significant and direct threat to the Union's public order and security" (Council of the EU, 2022). Their digital transmission is thus banned on the EU level as a whole.[4] The article focuses on sanctions that led to website blocking and network interference. Despite their generalisation and significant implications for human rights, the implementation of these

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

measures remains a vastly understudied area of research at the EU level, with the notable exception of Ververis et al. (2023).

While these sanctions can be categorised as an economic measure and the result of unexpected political developments, most notably the war in Ukraine, these sanctions must also be understood in the broader context of recent EU policies tackling online disinformation and foreign interference. While the EU has been aware of disinformation campaigns since the mid-2010s, it "gradually changed towards viewing disinformation as a threat to the EU's democratic foundations" in recent years (Kachelmann & Reiners, 2023). This public recognition favoured a political impetus for stronger legislative actions in this domain under the von der Leyen presidency of the European Commission.

These initiatives, exemplified by the recent EU Digital Services Act, the European Media Freedom Act and the Strategic Compass, also fit under the emerging umbrella of EU's digital sovereignty policies. These can, in turn, be understood as a new iteration of "Infrastructural Europeanism," the building of the Europe through infrastructure (Schipper & Schot, 2011). The discussions on tackling online disinformation and protecting Europe's digital sovereignty have simultaneously spiralled at the top of the European policy agenda at the end of the 2010s and early 2020s. Both reflect the identified need for better EU "resilience" in the face of the new threats posed by digital technologies. It needs to be acknowledged that in the EU's public discourse, "disinformation does not play a strong role in the digital sovereignty discussion," while "the concept and term of 'digital sovereignty' is not specifically mentioned in the most prominent EU policies against online disinformation" (Kachelmann & Reiners, 2023). Nevertheless, the war in Ukraine is known to have informed and inspired the acceleration of EU legislations both aimed at strengthening the EU's autonomy and capacity to control and protect its "cyberspace" and the spread of disinformation and foreign interference.[5]

This article aims to interrogate the actual effects of these new forms of sanctions, implemented at the infrastructure level of the internet, and reflect on their political implications for the EU's approach towards the internet and the enhancement of its digital sovereignty.

By linking two fields (sanctions and media policy) in which EU Member States retain considerable control and competencies, the formulation and implementation of sanctions targeting online broadcasters appears to be one of the least likely cases to observe manifestations of EU (digital) sovereignty. Yet, the recent quest of the Commission for a more geopolitical and digitally assertive agenda (Bonnamy & Perarnaud, 2023), as well as the nature and objectives of these measures, invite a careful investigation of their implications for the EU's digital sovereignty.

This article will thus answer the following research question: *How do sanctions aimed at internet infrastructure align with the EU's approach to internet governance and its digital sovereignty aspirations?*

To answer this question, we leverage internet measurements, policy analysis of EU documents, and the theoretical framework of infrastructural ideologies (Maxigas & ten Oever, 2023). We expand on the latter with the Althusserian notions of ideological and repressive state apparatuses (Althusser, 2014). This theoretical framework allows us to theorise the metagovernance of internet governance (Jessop, 2011; ten Oever, 2021),[6] in which the private transnational multistakeholder internet governance regime aims to increase interconnection between and among computing networks and users, while the national and multilateral internet governance regime aims to shape the network according to national and regional norms and values.

The lens of infrastructural ideologies and state apparatuses helps explain the bifurcated but dialectical relation between the multistakeholder and the multilateral internet governance regimes. This theoretical lens also explains the fit between digital sovereignty and the repressive state apparatus. Sovereignty works to exert control over local networks and thus

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

inscribe an asymmetrical end-to-end relationship in transnational networks (Zajácz, 2019) and limit foreign interference through repressive measures while maintaining interconnection. In other words, to limit direct foreign influence *on the content layer*. No country sufficiently controls the means for the reproduction of modern communication networks. Global supply chains for software and hardware and coordination of unique identifiers are too entangled to isolate countries and produce a genuinely sovereign stack. Furthermore, countries significantly benefit from transnational communications, and thus, complete sovereignty might not be desirable because of the higher costs and more friction that would result from it. The digital sovereignty discourse by the EU—and in this case, the sanctions as implementation thereof—is more of a tool of European coordination and integration and limitation of foreign information dissemination than an infrastructural disentanglement.[7]

The remainder of the article is structured as follows. The next section presents the methodological approach, drawing on unique network measurements and desk research. The results from the technical analysis will then be presented and contextualised in light of the EU digital policy agenda and the implementation of restrictive measures. Then, the article will discuss how these sanctions can be understood as both an instrument and challenge for EU digital sovereignty, followed by an exploration into what this may mean for the metagovernance of the internet.

METHODOLOGY

The study of the implementation and implications of EU restrictive measures aimed at Russian media outlets has been carried out using a multidisciplinary approach. It uses quantitative tools to apprehend the application of sanctions across EU Member States while also analysing the adoption and implementation process from a political perspective based on desk research and secondary sources.

For our analysis, we engaged in wide-ranging network measurements in different networks in several EU countries to understand the means and methods of the implementation of the sanctions.[8] The sanctions included in the scope of the study are presented in Table 1. This list draws from multiple authoritative sources and includes both Council decisions and national blocklists aimed at the Russian domain names that mirrored the German and Spanish-sanctioned websites of Russia Today (RT).

The technical analysis was aimed at understanding how access to select Russian resources may have been affected due to sanctions enforcement, focusing on connectivity and access to Russian media organisations from vantage points in Europe. To evaluate enforcement, we examined access across four broad dimensions: reachability, Domain Name System (DNS) response, Transport Layer Security (TLS) handshake, and Hypertext Transfer Protocol (HTTP) connection.

To accompany, frame, and contextualise the measurements, we have done extensive policy analysis of EU digital sovereignty documents and the policies and processes that have accompanied the sanction development and implementation. The political analysis drew on a literature review and the analysis of public documents from the EU and its Member States published from 2019—corresponding to the beginning of the von der Leyen presidency—until its end in 2024.[9]

This paper interrogates an inherently multidisciplinary topic, and it does so by using a variety of methods. This is important because infrastructures are inherently entangled with different parts of everyday life. However, this also presents a significant issue for the authors: methods speak to different literatures based on different understandings of the world (ontologies, as philosophers might say). In this paper, we do not resolve this issue. However, we seek to further the scholarship by combining qualitative and quantitative methods

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 1 List of sanctioned organisations, hostnames, and sources that formed the basis for measurements.

Sanctioned organisation	Hostname	Source	Remark/date added
Russia Today English	www.rt.com	Council decision 2022/351	March 01, 2022
Russia Today UK	www.rt.com	Council decision 2022/351	March 01, 2022
Russia Today Germany	de.rt.com	Council decision 2022/351	March 01, 2022
	deutsch.rt.com	Council decision 2022/351	March 01, 2022
Russia Today France	francais.rt.com	Council decision 2022/351	March 01, 2022
	fr.rt.com	Council decision 2022/351	March 01, 2022
RT en español	actualidad.rt.com	Council decision 2022/351	March 01, 2022
	actualidad-rt.com	Council decision 2022/351	March 01, 2022
Sputnik	www.sputniknews.com	Council decision 2022/351	March 01, 2022
	sputniknewslv.com	Council decision 2022/351	March 01, 2022
	sputniknews.gr	Council decision 2022/351	March 01, 2022
	sputniknews.cn	Council decision 2022/351	March 01, 2022
	radiosputnik.ria.ru	Council decision 2022/351	March 01, 2022
	sputnikglobe.com	Council decision 2022/351	Registered March 29, 2023, sputniknews. com now redirects to this domain name.
Rossiya RTR/RTR Planeta	www.rtr-planeta.com	Council decision 2022/884	June 03, 2022
	rtr-planeta.ru	Council decision 2022/884	June 03, 2022
	vgtrk.ru	Council decision 2022/884	June 03, 2022
Rossiya 24/Russia 24	www.vesti.ru	Council decision 2022/884	June 03, 2022
TV centre international	www.tvc.ru	Council decision 2022/884	June 03, 2022
	tvci.ru	Council decision 2022/884	June 03, 2022
NTV/NTV Mir	ntv.ru	Council decision 2022/2478	December 16, 2022
Rossiya 1	smotrim.ru	Council decision 2022/2478	December 16, 2022
REN TV	ren.tv	Council decision 2022/2478	December 16, 2022
Pervyi Kanal	1tv.ru	Council decision 2022/2478	December 16, 2022
RT Arabic	www.rtarabic.com	Council decision 2023/434	February 25, 2023
Sputnik Arabic	sputnikarabic.ae	Council decision 2023/434	February 25, 2023
RT en español mirror	esrt.online	Liwest blocklist	Registered April 08, 2022
	esrt.press	Liwest blocklist	Registered April 08, 2022
RT Germany mirror	rtde.site	Bundesnetzagentur	Registered March 05, 2022
	rtde.xyz	Bundesnetzagentur	Registered March 05, 2022
	rtde.team	Bundesnetzagentur	Registered March 05, 2022

(Continues)

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 1 (Continued)

Sanctioned organisation	Hostname	Source	Remark/date added
	test.rtde.live	Bundesnetzagentur	Registered April 06, 2022
	rtde.live	Bundesnetzagentur	Registered April 06, 2022
	test.rtde.website	Bundesnetzagentur	Registered April 06, 2022
	rtde.tech	Liwest blocklist	Registered April 06, 2022
	rtde.world	Liwest blocklist	Registered April 06, 2022
	rtde.me	Liwest blocklist	Registered April 06, 2022
A-Russia	a-russia.ru	Bundesnetzagentur	Russian TV streaming site
WWITV: World Wide Internet TV	wwitv.com	Bundesnetzagentur	TV streaming site
glaz.tv	www.glaz.tv	Bundesnetzagentur	TV streaming site
Russisches Fernsehen	www.russisches-tv-fernsehen.de	Bundesnetzagentur	TV streaming site
On TV time	ontvtime.tv	Bundesnetzagentur	TV streaming site
SPB TV World	spbtv.online	Bundesnetzagentur	TV streaming site
Coolstreaming	www.coolstreaming.us	Bundesnetzagentur	TV streaming site
Live HD TV	www.livehdtv.net	Bundesnetzagentur	TV streaming site
Rossiya segodnya group	snanews.de	Liwest blocklist	German news site
State Duma	duma.gov.ru	OFAC sanctions list	
Sberbank	www.sber-bank.by	Council decision 2022/327	February 25, 2022, Not part of Annex IX
	www.sberbank.ru	Council decision 2022/327	February 25, 2022, Not part of Annex IX
Gazprombank	www.gazprombank.ru	Council decision 2022/2478	December 16, 2022, Not part of Annex IX

from different fields and by building on the expertise of academic and non-academics from different backgrounds. The onto-epistemological disconnects in the paper can, in part, be attributed to the messy nature of politics, infrastructure, and reality.

LESSONS FROM THE HETEROGENEOUS TECHNICAL IMPLEMENTATION OF EU SANCTIONS

The results from the technical analysis underline how sanctions against Russian entities are inconsistently implemented across the EU in relation to the ban on certain media outlets.

Discrepancy in the enforcement of these measures can be justified first by the high-level description of the sanctions and the lack of recommendations for technical implementation. Indeed, the implementation of the sanctions was largely left to the interpretation of network

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

operators and guidance and interpretation provided by national authorities in EU Member States (if any). The sanctions did not describe how *operators* would need to prevent broadcasting by internet service providers, internet video-sharing platforms or applications.

In addition, though the design of sanction packages was led by the Commission, and in particular the cabinet of the Commission president (Håkansson, 2024), the application of EU sanctions was considered the prime responsibility of EU States. Thus, blocks were carried out in different ways, depending on the means, doctrine and policies of the country in question.

Table 2 presents measurement results between September 01, 2023 and September 05, 2023 per country and domain name. For each country, Table 2 reports the number of autonomous systems that are part of the scope of the study, along with the number of upstream resolvers and vantage points (VPs) covered. The significant number of vantage points (that we can equate to independent points of observation) highlights the depth and reliability of the measurements.[10] Each cell shows the share of responses that were not blocked. In other words, the proportion of resolvers that did not return an error or redirect. Overall, the results show that domain names that belong to organisations listed in the first

TABLE 2 Share of uncensored DNS responses received by RIPE Atlas probes relying on ISP upstream resolvers.

		Austria	Belgium	Bulgaria	Croatia	Cyprus	Czechia	Denmark	Estonia	Finland	France	Germany	Greece	Hungary	Ireland	Italy	Lithuania	Netherlands	Poland	Portugal	Slovakia	Slovenia	Spain	Sweden	United Kingdom	Switzerland	Russian Federation	United States
	# ASes	8	6	7	3	2	10	10	1	10	10	37	4	5	6	14	2	12	7	5	4	4	6	13	28	18	42	55
	# Upstream resolvers	25	22	11	5	5	34	19	2	21	78	205	7	7	16	33	3	53	19	8	7	9	14	37	103	59	79	229
	# VPs	64	138	28	9	5	57	56	5	73	573	656	21	26	62	115	4	245	34	247	10	15	63	52	192	222	108	661
Orgs listed by the EC	www.rt.com	7	1	9	0	0	38	33	0	2	2	25	0	14	13	23	0	5	28	0	0	0	34	100	81	99	96	98
	de.rt.com	6	1	9	0	0	30	31	0	2	4	25	9	14	28	97	0	6	44	0		0	68	94	81	100	100	98
	deutsch.rt.com	13	48	0	0	0	23	24	0	4	1	24	0	12	27	100	0	62	35	97	0	19	67	100	81	99	96	100
	francais.rt.com	4	3	0	0	0	21	25	0	2	3	26	22	14	22	34	0	6	46	0	0	19	70	100	80	99	90	98
	fr.rt.com	8	46	12	0	0	31	30	0	2	2	93	0	11	14	100	0	64	33	96	0	22	67	100	83	98	97	99
	actualidad.rt.com	19	1	7	0	0	31	32	0	0	3	25	9	12	23	100	0	6	43	0	0	0	66	95	83	100	88	99
	actualidad-rt.com	14	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	97	100	100	100	97	99
	www.sputniknews.com	4	8	9	0	0	33	26	0	6	0	30	0	73	16	31	0	3	87	0	0	0	100	95	80	100	88	99
	sputniknewslv.com	90	5	9	100	0	29	29	0	2	60	57	100	47	23	30	100	49	100	100	0	22	100	100	100	100	97	99
	sputniknews.gr	100	1	0	75	0	35	8	0	0	60	63	11	46	25	26	100	50	100	100	0	0	100	100	100	98	96	99
	sputniknews.cn	100	1	8	80	0	27	8	0	2	58	56	100	41	25	31	100	45	100	100	19	0	95	100	100	100	97	100
	radiosputnik.ria.ru	5	34	7	100		42	80	0	2	99	99	87	100	100	100	0	100	6	100	0	100	95	100	100	100	97	100
	sputnikglobe.com	100	100	100	100	100	100	100	100	7	100	99	100	100	100	100	100	100	100	100	100	16	100	100	100	100	89	100
	www.rtr-planeta.com	6	55	100	60	100	100	100	100	2	95	100	100	100	41	100	100	47	12	0	100	100	100	100	100	100	97	99
	rtr-planeta.ru	17	100	100	100	100	100	77	100	100	100	100	100	100	100	100	100	99	100	100	100	100	100	100	100	100	100	100
	vgtrk.ru	100	3	100	80	100	100	26	100	2	100	53	66	100	100	100	0	100	33	96	100	100	100	100	100	100	96	100
	www.vesti.ru	15	52	81	80	100	100	30	0	36	56	100	100	100	34	100	100	100	40	96	100	100	100	100	100	100	94	99
	www.tvc.ru	23	4	81	60	100	100	28	0	35	53	84	39	100	89	100	0	48	100	95	100	100	95	100	100	100	97	100
	ntv.ru	4	46	100	0	100	100	28	0	2	100	29	75	100	100	100	0	98	36	0	100	100	95	100	98	100	97	100
	smotrim.ru	100	58	100	19	100	100	30	0	2	57	31	50	100	18	100	0	100	33	0	100	100	95	100	100	100	97	99
	ren.tv	9	1	100	0	100	100	34	0	2	99	29	55	100	33	100	0	97	37	0	100	100	100	89	100	100	94	99
	1tv.ru	0	3	100	0	100	100	29	0	2	99	31	19	100	100	100	0	97	33	95	80	100	95	100	100	100	100	99
	ww.rtarabic.com	15	100	100	100	100	100	46	0	39	56	85	66	100	100	100	100	96	100	100	100	100	100	100	100	100	96	100
	sputnikarabic.ae	19	100	100	100	100	100	25	0	2	58	47	50	100	100	100	100	45	100	95	100	100	100	100	100	100	96	99
Mirror pages	esrt.online	17	100	100	100	100	94	100	100	100	99	99	100	92	100	100	100	100	100	100	100	100	100	100	100	100	94	99
	esrt.press	26	100	100	100		100	100	100	100	99	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
	rtde.site	14	100	100	100	100	100	76	100	100	99	28	75	100	100	100	100	100	100	96	100	100	100	100	100	99	100	100
	rtde.xyz	0	100	100	100	100	100	73	100	100	99	30	55	100	100	100	100	100	100	98	100	100	100	100	100	100	94	99
	rtde.team	0	100	100	100	100	100	73	100	100	100	32	50	100	100	100	100	100	100	98	100	100	100	100	100	100	96	99
	test.rtde.live	22	100	100	100	100	100	76	100	100	100	25	54	100	100	100	100	100	100	96	100	100	94	100	100	100	100	99
	rtde.live	18	98	100	100	100	100	76	100	100	99	98	92	100	100	100	100	100	100	100	100	100	95	100	100	93	97	100
	test.rtde.website	100	100	100	100	100	100	81	100	100	100	24	60	100	100	100	100	100	100	96	100	100	100	100	100	100	100	100
	rtde.tech	12	100	100	100	100	100	85	100	100	100	27	72	100	100	100	100	100	100	96	100	100	100	100	100	100	97	99
	rtde.world	35	100	100	100	100	100	78	100	100	99	29	63	100	100	100	100	100	100	94		100	100	100	100	100	100	99
	rtde.me	21	100	100	100	100	100	76	100	100	99	29	46	100	100	100	100	100	100	95	100	100	100	100	100	98	97	99
TV streaming svcs	a-russia.ru	100	100	100	60	100	94	86	0	100	100	30	50	100	100	100	0	100	100	95	100	100	100	100	99	100	100	98
	wwitv.com	100	100	100	100	100	100	43	100	88	100	28	28	100	100	100	0	100	100	94	100	100	100	100	100	100	100	100
	www.glaz.tv	100	100	100	60	100	100	81	0	97	100	43	60	100	100	100	0	100	100	96	100	100	100	83	99	100	100	100
	www.russisches-tv-fernsehen.de	100	100	100	60	100	100	100	100	100	100	100	100	100	100	100	0	100	100	100	100	100	100	100	100	100	96	99
	ontvtime.tv	100	53	100	60	100	100	31	0	88	100	31	71	100	25	100	0	100	100	95	100	100	100	100	100	99	100	100
	spbtv.online	100	100	100	100	100	100	100	0	100	100	32	50	100	100	100	0	100	100	97	100	100	100	100	100	100	97	100
	www.coolstreaming.us	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	92	99	100	97	99
	www.livehdtv.net	94	100	100	100	100	100	100	0	100	99	43	37	100	100	100	0	100	100	96	100	100	100	100	100	100	96	99
	snanews.de	15	1	9	100	25	50	28	100	2	59	31	28	15	26	83	100	86	100	94	0	30	100	100	100	100	96	100
Other	duma.gov.ru	100	100	100	100	100	100	81	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	97	99
	www.sber-bank.by	100	100	100	100	100	100	77	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	94	100
	www.sberbank.ru	100	100	100	100	100	100	85	100	100	100	100	81	100	100	100	100	100	100	100	100	100	96	100	100	100	100	100
	www.gazprombank.ru	100	100	100	100	100	100	78	100	100	100	100	100	100	100	100	100	100	100	100	100	100	95	100	99	99	97	99

Abbreviation: DNS, Domain Name System.

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Council decision are blocked more often than domain names added later. While there is some form of DNS blocking in all EU Member States, the extent to which blocking occurs differs widely from country to country and provider to provider.

Before the adoption of EU sanctions, it is interesting to note that some Member States had already taken actions against targeted Russian media outlets, namely Bulgaria, Germany, Estonia, Lithuania, Latvia and Poland (Cabrera Blázquez, 2022; Poli & Finelli, 2023). Though these prime-mover countries indeed appear to have more DNS blocking than the average, the level of implementation also remains relatively different among this group of States. Spain and Sweden account for the countries with the least DNS blocking among EU Member States, while Austria, Germany, Finland, Greece, Estonia, and Denmark are on the other end. Yet, even for countries with more maximalist approaches, it needs to be acknowledged that the implementation of the sanctions does not cover mirror pages (with the exception of Austria, Germany, Greece and Denmark), nor media streaming, and rarely targets all of the Russian media and organisations listed in Council decisions. Meaning that not just the technical implementation, but also the coverage of the sanctions implementation is heterogenous.

This is in coherence with the various and heterogeneous political responses to the invasion in EU Member States. Comparative analysis of how they each dealt with the media governance questions related to the informational dimension of the war has shown great discrepancies in the EU (Susi et al., 2022). For instance, several private broadcasters in Finland immediately suspended the distribution of Russian news channels, while in most other Member States, broadcasters and public authorities acted following the adoption of restrictive measures, with varying degrees of ambitions.

In addition to the contrasted implementation of the ban by EU Member States, several other challenges emerge from the technical analysis. Indeed, differences in the implementation also mean that when a page is blocked, there is no harmonised format to communicate with end users about these measures (See Figures 1 and 2). Usually, end users are not adequately informed that the reason they cannot access the requested resource is due to EU-mandated filtering. When users are informed, the way this is done is not uniform. Some block pages only indicated that the page was blocked (or not accessible due to maintenance), while others provided a full list of all web pages that were blocked by this provider. Another provider gave all possible reasons why a website could be blocked, and some pages informed the user about the applicable EU decision that led to the blocking of this web page. This makes it hard for end-users to understand the specific reasons why a resource is blocked, let alone have access to use their right to appeal. This negatively impacts the democratic legitimacy of these EU measures in their implementation (Schmidt, 2013).

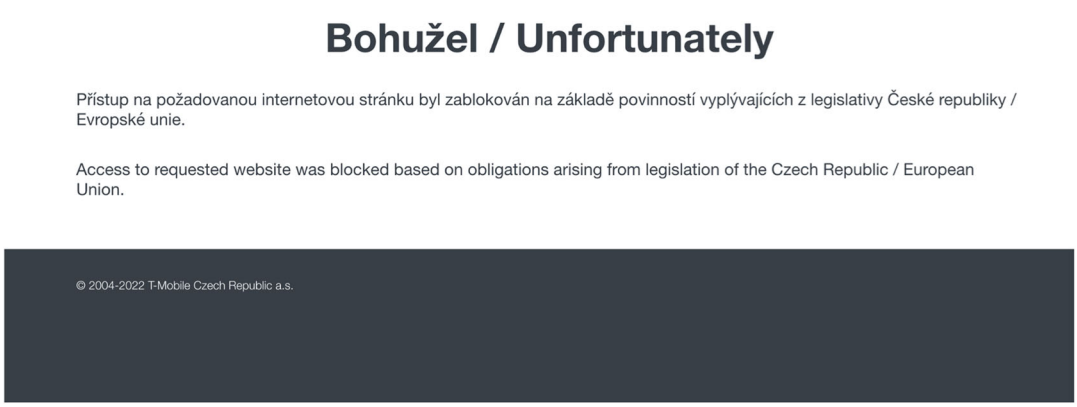

FIGURE 1 Instance of a block page from T-Mobile Czech Republic in 2022.

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Šiuo metu nėra galimybės pasiekti šios svetainės, nes joje buvo nustatyta neteisėtai vykdoma veikla – apie joje vykdomą televizijos programų ir (ar) atskirų programų platinimo internete Lietuvos Respublikos vartotojams veiklą nebuvo pranešta Lietuvos radijo ir televizijos komisijai teisės aktų nustatyta tvarka.

Informaciją apie asmenų, neteisėtai vykdančių televizijos programų ir (ar) atskirų programų platinimo internete Lietuvos Respublikos vartotojams, veiklą galite rasti čia.

Dėl išsamesnės informacijos prašome kreiptis į Lietuvos radijo ir televizijos komisiją,

tel. (8 5) 233 0660, faks. (8 5) 264 7125, e. p. lrtk@rtk.lt.

You have been redirected to this website, because at present there is no access to the website you are trying to reach because of illegal services detected on that website, i.e. the services of the distribution of television programmes and (or) individual programmes on the Internet for the users of the Republic of Lithuania were not notified to the Radio and Television Commission of Lithuania in accordance with the procedure established by legal acts.

Information on the illegal services of the distribution of television programmes and (or) individual programmes on the Internet for the users of the Republic of Lithuania is provided here.

For more information, please contact the Radio and Television Commission of Lithuania,

tel. +370 5 233 0660, fax. +370 5 264 7125, e-mail: lrtk@rtk.lt.

FIGURE 2 Instance of a blockpage from the Radio and Television Commission of Lithuania in 20.

Also, despite the efforts of most EU Member States, the analysis indicates that it is still very easy to find content from Russia Today and Sputnik online, both through mirror sites and aggregate sites. Regarding mirror pages, in response to DNS-based sanctions, new Russian domain names were registered that mirrored the German and Spanish-sanctioned websites of Russia Today.

Table 2 shows that these new mirror pages are only sometimes blocked in most countries. For example, Spanish sites are only blocked by Austrian providers, but they are not blocked in Spain as we would have expected. On the other hand, German mirror pages are blocked by most providers in Austria and Germany, with some exceptions. Measurements for VPs in one Portuguese network indicate that some of the mirrored domain names are blocked only part of the time.

This evidence challenges the *suitability* of recent sanction packages to address online foreign interference and disinformation. From a technical perspective, these measures were enforced very heterogeneously, and these discrepancies induce a form of arbitrariness.

The findings of the technical analysis thus underline the disconnect between the EU political approach and the complexity of the technical measures needed to enforce those sanctions. This ironically mirrors the discrepancy between the claims of the Russian surveillance apparatus for censorship and traffic interception and the actual implementation of those measures and systems in reality by internet actors (Ermoshina et al., 2022).

This state of play questions what is known to be one of the most fundamental transformations in the formulation and implementation of sanctions at the EU level (Meissner & Graziani, 2023). Indeed, after decades of a decentralised approach, the Commission has

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

pushed for more uniformity in the enforcement and implementation of sanctions across Member States through a more centralised approach (Portela, 2024). The war in Ukraine has further accelerated this transfer of competence to the EU level, for instance, illustrated by the new Commission's "freeze and seize" task force for the freezing and confiscation of assets owned by individuals and entities targeted by such sanctions (European Commission, 2022).

However, this quest for uniformity appears to be greatly limited in our case by the limited coordination of national regulators in this new realm for sanctions and the inherent technical obstacles posed by such blocking on internet infrastructures. In the following section, we will investigate what this assessment of the technical implementation of sanctions may mean for EU digital sovereignty.

SANCTIONS AS AN INSTRUMENT AND CHALLENGE FOR THE EU'S APPROACH TO THE INTERNET

The war in Ukraine is known to have informed and inspired the acceleration of EU legislations aimed at strengthening the EU's capacity to protect its "cyberspace" against the spread of disinformation and foreign interference, which the European Commission has equated to its "digital sovereignty."

Many authors have claimed the predominant discursive nature of digital sovereignty policies in the EU. While sanctions are nowhere mentioned as a tool of digital sovereignty per se, we argue that sanctions could be interpreted as one of the first techno-material digital sovereignty measures.

In this section, we present how sanctions in the context of the Russian invasion of Ukraine have contributed to strengthening the Commission agenda on the EU's digital sovereignty. At the same time, we interrogate the traditional pillars of the EU's approach to the internet, both from an infrastructural (*fragmentation*) and legal (*freedom of expression*) perspectives. As we will see, those challenges also lead to new discussions on how internet sanctions could be improved.

Sanctions as a catalyst for the Commission's policy agenda

Meissner and Graziani have shown that sanction design has been a tool recently mobilised by the Commission to assert itself in the geopolitical arena and in a policy domain traditionally controlled by Member States (Meissner & Graziani, 2023). This is not surprising since sanction formulation at the European level, particularly in moments of crisis, provides an opportunity structure beneficial to the Commission for several reasons. First, individual States tend not to impose sanctions autonomously (Giumelli & Lavallée, 2013), but also because of the coordination capabilities required to formulate decisions to be adopted unanimously by 27 Member States in a very short timeframe - a setting which gradually pushed the Commission in the driving seat following the Russian invasion. This instance shows how Member States now rely on the EU level and the Commission to adopt sanctions—showing how their formulation has gradually become a normalised exercise of "EU sovereignty" (Roch & Oleart, 2024).

The observation that the Commission has experienced some level of success in pursuing its digital sovereignty agenda in this domain, with varying levels of success in other fields (Perarnaud & Rossi, 2023), can be attributed to the particular political opportunity structure afforded by the Russian aggression against Ukraine which aligned the Commission and the Member States represented in the European Council. Previous endeavours of

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

the Commission suffered from a bifurcated approach, namely strengthening the European industry while maintaining openness, global interconnection, integration, and market access. This appeared to hamper the effectiveness of previous interventions. These attempts were in part hindered by the dual interests of EU Member States, which wanted to benefit from a strong Europe to foster their own "European champions" while remaining integrated into a global economy with complex global supply lines and communication infrastructures.

In this case of Russia's aggression against Ukraine, EU Member States, as well as the European Commission, were aligned in their position vis-a-vis Russia, namely to limit the impact of Russian media infrastructural connectivity to Europe. The war against Ukraine convinced the Member States and the Commission that economic, scientific, cultural, defence, diplomatic and sportive ties with Russia (the traditional fields of sanctions) should be leveraged; therefore, their position in the European Council to limit ties with Russia aligned with the interest of achieving digital sovereignty of the Commission. In other words, the establishment of digital sovereignty was facilitated through exogenous pressures that allowed for the internal alignment of different parts of European law and policymaking to limit.

In relation to the digital realm, the Commission is becoming the power centre concerning the imposition of sanctions directed towards internet infrastructures, thus adding a new lever to its repertoire of action to strengthen the EU's digital sovereignty. Rather silently, however, as digital sovereignty has not emerged as a central reference point (Falkner et al., 2024) in the field of EU sanctions partly because the ban on Russian media outlets was discussed from the perspective of media law.

Internet fragmentation and EU sanctions

The adoption and implementation of these sanctions have directly affected current debates on the fragmentation of the internet (Perarnaud et al., 2022). Indeed, they could trigger and normalise a wave of subsequent decisions applied to other countries that could foster a regime with differentiated approaches to regions of the world. A process that some might identify as a high-level form of fragmentation of the internet by directly impeding connectivity between the EU and other third countries.[11]

As part of the negotiation of sanction packages, EU Member States and institutions discussed whether sanctions should also cover key internet resources that are, for some, managed by entities under EU jurisdiction.[12] The Netherlands is, for instance, the host country of RIPE NCC, the IP registry for Europe, the Middle East and Former Soviet Union countries. According to the Dutch Ministry of Foreign Affairs (Fragkouli, 2021), the registration of internet number resources (such as Autonomous System Numbers and IP addresses) is considered to be an economic resource. This means that when sanctions are adopted, RIPE NCC needs to ensure that sanctioned entities cannot receive new resources or trade their existing ones. The Dutch government, however, also confirmed that some assets held by sanctioned parties do not need to be deregistered (ibidem).

Interestingly, the EU passed an amendment to the sanctions on June 3, 2022, indicating that the sanctions: '… *shall not apply to funds or economic resources that are strictly necessary for the provision of electronic communication services by Union telecommunication operators, for the provision of associated facilities and services necessary for the operation, maintenance and security of such electronic communication services, in Russia, in Ukraine, in the Union, between Russia and the Union, and between Ukraine and the Union, and for data centre services in the Union, as well as international payments for internet*'.[13] This means that Russian internet providers, despite the EU sanctions, can still

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

use their network numbers and IP addresses. In other words, the EU and its Member States have made sure to avoid facilitating internet fragmentation on the interconnection level of the internet.

Instead, a legal basis was found in EU media and broadcasting legislation to block the media outlets Russia Today and Sputnik because of the content they distributed.[14] Technical blocking was, therefore, a means to the end of preventing the dissemination of content. While this study shows that the blocking of content was not homogeneously or meaningfully achieved, it is also hard to qualify this as internet fragmentation on the interconnection level. This is because the filtering is done by *local bodies* and is only applied to *local networks*. The blocking of Russia Today in the EU does not intend to limit the dissemination of Russia Today outside of the EU. While practices of DNS filtering and forms of geoblocking have been qualified as factors of internet fragmentation in the past (Drake et al., 2016), the limited scale of the blocking (both in terms of sanctioned sites and territorial scope), adding to the presumed temporary nature of the blocking, seriously downplay concerns of internet fragmentation on the interconnection level in this case.

The emergence of network blocking promoted by the EU with these sanctions instead resembles the early internet adage of: 'my network, my rules'. Countries can set their own rules for the edge or access networks in their territory, and it appears thus far-fetched to call this internet fragmentation on a technical level as long as they continue to respect rules for interconnection and do not hamper other networks from doing the same.

The complex articulation of infrastructure sanctions and the rule of law

This train of sanctions aimed at internet infrastructure, infrastructure sanctions in short, also questions another key dimension of the EU's approach to the internet, related to fundamental rights and freedom of expression.

In recent digital policy and internet governance literature, the EU approach is regularly described as a "right-based approach" (Bradford, 2023). While sanctions are often used as an instrument against human rights violations, they can also negatively impact human rights (Peksen, 2009). This is why it is of crucial importance to analyse this instrument on its potential impact on freedom of expression and access to information, as well as due process.

Though recently considered legal by the French Council of State and the General Court of the EU,[15] following a challenge by Russia Today, the legal soundness of this suspension has been vividly discussed, especially given the concerns that it could normalise the "excessive over-blocking of websites and services" (Ververis et al., 2023).

Several countries in Europe (such as Switzerland and Norway) decided to abstain from suspending Russian media, and in particular Norway, on the ground that it would "constitute an unjustified interference in freedom of expression" (Hofer, 2023). In a recent case, the Grand Chamber of the General Court dismissed RT France's application for annulment of acts of the Council on the ground that the broadcasting ban did not constitute interference with the essence of freedom of expression in part because it was temporary and reversible. Yet, this judgement remains, for some, controversial as it "remains to be seen whether the perception of the threat to the Union's public order and security posed by the disinformation campaign of Russian media outlets will change after the end of the war" (Poli & Finelli, 2023). One can indeed question the temporary nature of those restrictions.

Our technical analysis also provides relevant insights in terms of transparency and due process. When pages by the sanctioned media are blocked, this happens in a wide variety of manners, as described above. In the 125 network vantage points where we observed DNS-style blocking, only 32 of them showed a block page. The lack of information as to why a

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

website is blocked makes it very hard for most users to understand why a website is blocked, hampering their right to remedy and access to due process if they feel this website is unduly filtered. It might even give users the impression that Russia itself is blocking access to information in the EU. Our findings show that this hampers the ability of citizens to understand the impact of EU policies on their fundamentals and human rights to access information and freedom of expression (Kulesza, 2014).

The Russian invasion of Ukraine has had clear ripple effects on the EU's policy agenda since 2022. A key provision was, for instance, added at the last minute during the negotiation of the Digital Service Act to include a crisis response mechanism directly inspired by the challenges raised by the Russian invasion. Some of the recent EU policy discussions have thus aimed to address the limitations of the sanction tools aimed at Russian media. This is illustrated, for instance, by the 2024 European Media Freedom Act and its mechanism for the coordination of measures concerning media service providers outside the EU. It has been adopted to mitigate the over-reliance of the EU on sanctions to curb the access to an EU audience to certain media providers in view of their "serious and grave risk of prejudice to public security and defence." According to Cole and Etteldorf (2023), this provision can be interpreted as a "reaction to difficulties observed when trying to achieve a common reaction to the risks created by dissemination of Russian channels in the EU after the Russian Federation started war against Ukraine."

While the previous parts underline the limits and negative externalities that have characterised the implementation of these infrastructure sanctions, the following one highlights that this also gave rise to a new discussion on how to improve internet sanctions.

Can internet sanctions be improved?

When Andrii Nabok (Андрій Набок) and Deputy Prime Minister Mykhailo Fedorov (Михайло Федоров) of the Ukrainian Ministry of Digital Transformation sent a letter[16] addressed to the Internet Corporation for Assigned Names and Numbers (ICANN) and RIPE NCC on the morning of Monday, February 28, 2022, they got a quick a univocal response from ICANN[17] and RIPE NCC,[18] saying that they would not answer their request. On the contrary, RIPE NCC's Executive Board wrote that it "believes that the means to communicate should not be affected by domestic political disputes, international conflicts or war"[19] and that it was "committed to taking all lawful steps available to ensure that the RIPE NCC can provide undisrupted services to all members across our service region and the global internet community."[20] In other words, it would do everything to keep on serving Russia, the actor that was at that very moment attacking Ukrainian communications infrastructure (Luconi & Vecchio, 2022).

Several parts to the responses by internet multistakeholder governance bodies need to be highlighted. First, while RIPE NCC and ICANN generally pride themselves on their extensive multi-stakeholder processes, where community members engage in long and very proceduralized joint policy development processes, the leadership of both organisations visibly thought this was not necessary in this case.

RIPE NCC stated that it "is crucial that the RIPE NCC remains neutral and does not take positions concerning domestic political disputes, international conflicts or war."[21] The ICANN President and CEO further added that: "*[W]ithin our mission, we maintain neutrality and act in support of the global Internet. Our mission does not extend to taking punitive actions, issuing sanctions, or restricting access against segments of the Internet – regardless of the provocations. ICANN applies its policies consistently and in alignment with documented processes. To make unilateral changes would erode trust in the multistakeholder model and the policies designed to sustain global Internet interoperability.*"[22]

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

ICANN and RIPE NCC clearly emphasised they wanted to support the global internet by maintaining and increasing interconnection. ICANN described that restricting access would fall outside its mission, while RIPE NCC added that it will take "all lawful steps available to ensure that the RIPE NCC can provide undisrupted services to all members across our service region and the global internet community." ICANN and RIPE NCC, as global bodies, wanted to prevent the politicisation of the governance of global interconnection.

Similarly, the EU seemed to follow this reasoning and not address the interconnection level of the internet through its sanctions but rather access to websites *within its own borders.* Here, the ambitions of the EU's digital sovereignty differ from the extra-territorial aspirations of the General Data Protection Regulation (GDPR). Where the GDPR also applies to EU citizens outside of the EU, these internet sanctions have a territorial scope (Lambach, 2019) and apply to access networks in the European Union. Our technical analysis reminds us, however, that the actual implementation of these sanctions differs widely across networks for various political and technical reasons. At least in part, this can be attributed to the practice that laws and directives are defined in technological neutral ways, which means that "legislation should define the objectives to be achieved, and should neither impose nor discriminate in favour of, the use of a particular type of technology to achieve those objectives" (Ali, 2009, p. 8). This leaves a lot of space for guidance per nation-state, which in part contributes to the diffuse implementation that this research shows. The European Commission still has to publish its evaluation of the implementation and effectiveness of these sanctions.

This section shows that the EU, through these infrastructure sanctions, has chosen to limit its influence to the content layer of the internet while leaving the interconnection layer untouched. The sanctions and the policy debates that ensued within the broader internet governance community demonstrate how the EU's digital sovereignty approach is structurally limited by the entanglement of internet "resources" at the global scale. This is true both materially and ideologically, as will be developed in the next section drawing on the concept of "infrastructural ideology" (Maxigas & ten Oever, 2023).

EXPLAINING THE DISCONNECT: STATE APPARATUSES OF IDEOLOGY AND REPRESSION IN THE METAGOVERNANCE OF THE INTERNET INFRASTRUCTURE

This case of European sanctions aimed at internet infrastructures is a very useful site to observe the making and implications of the EU's digital sovereignty approach for other fields of power, including "internet governance." It shows how the EU directly legitimises the permanence of a particular "order" for the internet (or, in other words, an ideology), cognisant of its own interests and constraints in relation to the global internet infrastructure. As a result, we explore in this section what drives the shaping of the EU's digital sovereignty, reflecting on the articulation between these two ideological and infrastructural dimensions.

Of ideology and infrastructure

In his book "Valences of the Dialectic," Frederic Jameson (2020) explains that every time generates its version of ideology, and therefore also of ideology critique. Ideology is what generally is understood as "common sense," things that are not questioned but that structure our everyday life.

In this sense, ideology is very similar to infrastructure. Infrastructures, as Susan Leigh–Star and Bowker wrote, are "technologies and arrangements that, by design and by habit,

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

tend to fade into the woodwork" (Bowker & Star, 2000, p. 34). The difference that thus far has been made between ideology and infrastructure is that—generally speaking—ideology was understood as discursive and infrastructure as material. However, as we will explain, the concept of infrastructural ideology (Maxigas & ten Oever, 2023) helps bridge the two realms, which is particularly apt for the current time with its own ideology.

The social geographer Keller Easterling writes that: "Some of the most radical changes to the globalizing world are being written, not in the language of law and diplomacy, but rather in [. .] infrastructural technologies" (Easterling, 2014, 15). She writes this not because technology has all of a sudden been imbued with extraordinary power, but rather that communication infrastructures are interconnected across the globe, at the same time that global multilateral processes in the languages of (international) law and diplomacy are breaking down.

In other words, communication infrastructures are the main means of connection in the world. While in previous wars, the first thing that would happen would be the cutting of telegraphic cables (Zajácz, 2019), in the war in Ukraine, we see that networks are being reconfigured but continue to be interconnected through the global internet (Fontugne et al., 2020; Limonier et al., 2021).

Explaining the permanence of interconnection

In an era that is characterised by deglobalisation, or de-coupling, the emergence of digital sovereignty discourse, and the resurgence of international armed conflict between States and power blocks, it is quite remarkable that interconnection persists. Not only does it persist, but communication networks rapidly develop and get reconfigured to address challenges, and in the meantime, internet traffic and connected devices keep growing. For the internet, the reproduction of the conditions of production does not just maintain itself but aligns and increases productive forces and the existing relations of production. This means that there is an ideological state apparatus, a plurality of organisations and relations that are not formally part of the state, that produce the preconditions for internet connectivity. This ideological state apparatus that produces interconnection is private multistakeholder internet governance.

Multistakeholder internet governance produces global interconnectivity by continuously testifying that it is politically neutral. This was exactly the message from ICANN and RIPE NCC: their goal is to maintain and increase interconnection and not meddle with political conflicts. The only aim of multistakeholder internet governance is to increase interconnection by aligning transnational economic forces and relations of production through the provision of a political superstructure through a particular mode of global governance (ten Oever, 2021). It does so by maintaining the culture of specific epistemic communities, such as in internet standard setting (Abbate, 1999; Cath, 2021; Russell, 2014).

An ideological state apparatus, however, cannot exist without being connected to a repressive state apparatus (Althusser, 2014). In an emerging multipolar world, (blocks of) nation-states seek to inscribe their norms and values in global communication networks and seek to limit the control of other (blocks of) nation-states. However, not a single block aims to produce its technological stack. Here we see the metagovernance, or the governance of governance, between the ideological state apparatus of multistakeholder internet governance and the regimes of repressive state apparatuses.

In this, sanctions have the role of an instrument of an emergent repressive state apparatus. The European Union is emergent as a repressive state apparatus because it is currently only used to control content, not networks or their interconnection, and always toeing the line between supranationalism and intergovernmentalism. But exactly when Russia emerged as an enemy of both the EU Member States as well as the European Commission, this allowed the latter to implement its agenda of digital sovereignty, but solely

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

in a technologically neutral manner and only on higher levels of the technological stack where it did not endanger network interconnection.

To ensure this was understood, payments for network (inter)connectivity were exempt from the sanctions. This opportunity allowed the material shaping of EU digital sovereignty that thus far had remained largely discursive. But it did not impede upon the technical interconnection level, which is the purview of the ideological state apparatus, which does have direct control over the means of production of interconnection.

CONCLUSION

In this article, we have framed the recent sanctions against Russian media as being (silently) part of the digital sovereignty approach of the European Union and reflected upon their implications for the EU's broader engagement with internet governance. From our analysis, we can derive three main contributions.

First, based on a series of unique and comprehensive network measurements, we found that these EU sanctions against Russian media have been inconsistently implemented across the EU. Also, when content is blocked, the user is not always informed, while much of the blocked content can be found on mirror sites that are largely available on the European continent. The inconsistent implementation of the sanctions can, at least in part, be attributed to the high-level and technology-neutral description of the sanctions and the lack of recommendations for technical implementation. The lack of (correct) information on the reasons for the blocking of content has a negative impact on the democratic legitimacy of the measure.

Second, despite their heterogeneous implementation, these sanctions have contributed to the strengthening of the Commission's agenda to foster the EU's digital sovereignty. At the same time, they clearly echo some of the long-standing pillars of the EU's approach to the internet, both from infrastructural and legal perspectives. We show that the EU, through these infrastructural sanctions, has chosen to limit its influence to the content layer of the internet while leaving untouched the interconnection layer, mirroring the resistance of other multistakeholder organisations (such as RIPE NCC and ICANN) towards other sanctions and interpreting the limitation of connectivity outside of their mandate.

Third, expanding on this case, we theorise the response to Russia's aggression in Ukraine as the emergence of an EU digitally sovereign repressive state apparatus (Althusser, 2014) implementing sanctions. Meanwhile, the ideological state apparatus of multistakeholder internet governance limits itself to increasing interconnection and connectivity, which is its infrastructural ideology that gets embedded in technology, governance bodies, processes, procedures, and the culture of its epistemic communities.

The distinction between the repressive and ideological state apparatuses explains why there is no real technical fragmentation happening. The ideological state apparatus of multistakeholder internet governance maintains the interconnection layer of the stack, which remains explicitly untargeted by the sanctions. The emerging EU repressive state apparatus, at the same time, aims to limit foreign influence and seeks to inscribe its norms and values in the networks as a manner of selective interconnectivity (Huang et al., 2022).

Future research could seek to apply the framework of metagovernance of internet governance between the global ideological state apparatuses and (different) repressive state apparatuses to test its relevance and validity. We expect it will help explain how the different regimes are complementary with different means and methods rather than merely competing for network control. Multistakeholder internet governance aims to be politically neutral to accommodate the politics that different repressive state apparatuses can apply to their networks. The repressive state apparatuses define their demands in a technologically neutral way so that the multistakeholder internet governance can continue to develop and adapt.

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

ACKNOWLEDGMENTS

This project was made possible by the Ford Foundation, the Internet Society Foundation, and the Open Technology Fund. An earlier version of this paper was presented at FOCI and has been printed in their proceedings.

ORCID

Niels ten Oever http://orcid.org/0000-0001-5134-2199
Clement Perarnaud http://orcid.org/0000-0002-6491-1466

ENDNOTES

[1] We refer to Internet infrastructures not only as the physical space of routers, data centers and submarine cables, but also to "all the choices, devices, configurations, relations, and characteristics" continuously shaping them (ten Oever, 2020).

[2] Only in a few exceptional cases, including this one, Treaty provisions can directly apply (Cabrera Blázquez, 2022).

[3] Known in EU jargon as *restrictive measures*.

[4] According to Poli and Finelli (2023), "the Council does not qualify disinformation activities as propaganda for war prohibited under Art. 20(1) ICCPR; however, their destabilising effect on the Member States and the neighbours is enough to qualify them as 'a significant and direct threat to the Union's public order and security'. It is the first time that the EU has defended such an interest".

[5] This applies for instance to a series of legislative texts aimed at enhancing the EU's cybersecurity, such as the Digital Operational Resilience Act (DORA), the revised Network and Information Security Directive (NIS2) or the Cyber Resilience Act (CRA).

[6] For an extensive discussion of the terms metagovernance and its application to internet governance, see the aforementioned sources.

[7] As will be illustrated through the reactions by RIPE NCC and ICANN below.

[8] A detailed description of the measurement approach can be found in Appendix S1.

[9] The policy documents in the scope of the literature review include EU statements and Council conclusions in relation to digital matters and Internet governance from 2019, the various packages of European sanctions adopted against Russia since 2022, as well as relevant national measures and laws from Member States.

[10] The measurements in this case rely on RIPE Atlas, a global network of probes that measures Internet connectivity and reachability.

[11] Though there is no general agreement about what Internet fragmentation may mean in practice, we use the definition proposed by Perarnaud et al. (2022), according to which technical fragmentation is "the result of choices that intentionally or unintentionally break, restrict or suspend technical connectivity between a part of the internet and the rest of the network".

[12] Council Regulation (EU) 2022/880 of June 3, 2022 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0880&from=EN accessed on July 2, 2024.

[13] Council Regulation (EU) 2022/880 of June 3, 2022 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0880&from=EN accessed on February 29, 2024.

[14] https://rm.coe.int/note-rt-sputnik/1680a5dd5d accessed on July 2, 2024.

[15] Judgement of the General Court in Case T-125/22. URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-07/cp220132en.pdf accessed on July 2, 2024.

[16] https://pastebin.com/DLbmYahS accessed on February 26, 2024.

[17] https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf accessed on February 26, 2024.

[18] https://www.ripe.net/publications/news/ripe-ncc-executive-board-resolution-on-provision-of-critical-services/ accessed on February 26, 2024.

[19] Ibidem.

[20] Ibidem.

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

[21] Ibidem.

[22] https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf accessed on February 26, 2024.

REFERENCES

Abbate, J. (1999). Inventing the internet, *Inside technology*. The MIT Press.

Ali, R. (2009). Technological neutrality. *Lex Electronica*, *14*(2), 1–15.

Althusser, L. (2014). *On the reproduction of capitalism: Ideology and ideological state apparatuses*. Verso Books.

Bonnamy, C., & Perarnaud, C. (2023). Introduction. EU digital policies and politics: Unpacking the european approach to regulate the "digital". *Politique Européenne*, *81*, 8–27. https://www.cairn.info/revue–2023-3-page-8.htm

Bowker, G. C., & Star, S. L. (2000). *Sorting things out: Classification and its consequences*. The MIT Press.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press. https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=3662601

Cabrera Blázquez, F. J. (2022). *The implementation of EU sanctions against RT and Sputnik*. Council of Europe. https://rm.coe.int/note-rt-sputnik/1680a5dd5d

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

Cath, C. (2021). The technology we choose to create: Human rights advocacy in the Internet engineering task force. *Telecommunications Policy*, *45*(6), 102144. https://doi.org/10.1016/j.telpol.2021.102144

Cole, M. D., & Etteldorf, C. (2023). *Future regulation of cross-border audiovisual content dissemination: A critical analysis of the current regulatory framework for law enforcement under the EU audiovisual media services directive and the proposal for a European Media Freedom Act*. Nomos.

Council of the European Union. (2022). *Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*.

Drake, W. J., Vinton, C. G., & Kleinwächter, W. (2016). *Internet fragmentation: An overview*. World Economic Forum.

Easterling, K. (2014). *Extrastatecraft: The power of infrastructure space*. Verso Books.

Ermoshina, K., Loveluck, B., & Musiani, F. (2022). A market of black boxes: The political economy of internet surveillance and censorship in Russia. *Journal of Information Technology & Politics*, *19*(1), 18–33. https://doi.org/10.1080/19331681.2021.1905972

European Commission. (2022). *Enforcing sanctions against listed Russian and Belarussian oligarchs: Commission's "Freeze and Seize" Task Force steps up work with international partners*. European Commission.

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty—Rhetoric and reality: Special issue framework paper. *Journal of European Public Policy*, *31*(8), 2099–2120.

Fontugne, R., Ermoshina, K., & Aben, E (2020). The internet in crimea: A case study on routing interregnumIn*2020 IFIP Networking Conference*. IEEE.

Fragkouli, A. (2021). *How sanctions affect the RIPE NCC. RIPE Labs*. RIPE Labs. https://labs.ripe.net/author/athina/how-sanctions-affect-the-ripe-ncc/

Giumelli, F., & Lavallée, C. (2013). Introduction—EU security governance: From processes to policies. *Journal of Contemporary European Research*, *9*(3), 390–405.

Håkansson, C. (2024). The Ukraine war and the emergence of the European commission as a geopolitical actor. *Journal of European Integration*, *46*(1), 25–45.

Helberger, N., & Schulz, W. (2022). Understandable, but still wrong: How freedom of communication suffers in the zeal for sanctions. LSE Media Blog. https://blogs.lse.ac.uk/medialse/2022/06/10/understandable-but-still-wrong-how-freedom-of-communication-suffers-in-the-zeal-for-sanctions/

Hofer, A. (2023). The EU's 'massive and targeted' sanctions in response to Russian aggression, a contradiction in terms. *Cambridge Yearbook of European Legal Studies*, *2023*, 1–21. https://doi.org/10.1017/cel.2023.9

Huang, Y., Huppenbauer, N., & Mayer, M. (2022). Infrastructuring cyberspace: Exploring China's imaginary and practices of selective connectivity. *International Quarterly for Asian Studies*, *53*(3), 413–439. https://doi.org/10.11588/iqas.2022.3.13947

Jameson, F. (2020). *Valences of the Dialectic*, Verso books.

Jessop, B. (2011). Metagovernance. In M. Bevir, *Handbook of Governance* (pp. 106–123). Sage.

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*, 11–36. https://doi.org/10.3917/eufor.396.0011

Kulesza, J. (2014). Freedom of expression on-line: Rights and responsibilities of internet service providers. *International Journal of E-Politics (IJEP)*, *5*(4), 52–65. https://doi.org/10.4018/ijep.2014100103

Lambach, D. (2019). The territorialization of cyberspace. *International Studies Review*, *22*(3), 482–506. https://doi.org/10.1093/isr/viz022

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Limonier, K., Douzet, F., Pétiniaud, L., Salamatian, L., & Salamatian, K. (2021). Mapping the routes of the internet for geopolitics: The case of eastern Ukraine. *First Monday*, *26*(5). https://doi.org/10.5210/fm.v26i5.11700
Luconi, V., & Vecchio, A. (2022). Impact of the first months of war on routing and latency in Ukraine. *arXiv*, *224*. https://doi.org/10.48550/arXiv.2208.09202
Maxigas, M., & ten Oever, N. (2023). Geopolitics in the infrastructural ideology of 5G. *Global Media and China*, 20594364231193950. https://doi.org/10.1177/20594364231193950
Meissner, K., & Graziani, C. (2023). The transformation and design of EU restrictive measures against Russia. *Journal of European Integration*, *45*(3), 377–394. https://doi.org/10.1080/07036337.2023.2190105
ten Oever, N. (2020). *Wired Norms: Inscription, resistance, and subversion in the governance of the Internet infrastructure* [PhD thesis, University of Amsterdam].
ten Oever, N. (2021). Norm conflict in the governance of transnational and distributed infrastructures: The case of Internet routing. *Globalizations*, *1*, 17.
ten Oever, N. (2021). The metagovernance of internet governanceIn B. Haggart, N. Tusikov, & J. Scholte, *Contested power and authority in internet governance: Return of the state?* Routledge.
Olsen, K. B. (2022). Economic power, geoeconomics, and sanctions, *The geoeconomic diplomacy of European sanctions* (pp. 16–43). Brill Nijhoff.
Peksen, D. (2009). Better or worse? The effect of economic sanctions on human rights. *Journal of Peace Research*, *46*(1), 59–77.
Perarnaud, C., & Rossi, J. (2023). The EU and internet standards—Beyond the spin, a strategic turn? *Journal of European Public Policy*, *31*(8), 2175–2199. https://www.tandfonline.com/doi/abs/10.1080/13501763.2023.2251036
Perarnaud, C., Rossi, J., Musiani, F., & Castex, L. (2022). Splinternets': Addressing the renewed debate on internet fragmentation." Panel for the Future of Science and Technology, Scientific Foresight Unit (STOA). *European Parliamentary Research Service*. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729530/EPRS_STU(2022)729530_EN.pdf
Poli, S., & Finelli, F. (2023). Context specific and structural changes in EU restrictive measures adopted in reaction to Russia's aggression on Ukraine. *Eurojus*, *3*.
Portela, C. (2024). Sanctions and the geopolitical commission: The war over Ukraine and the transformation of EU governance. *European Papers - A Journal on Law and Integration*, *2023*(3), 1125–1130.
Roch, J., & Oleart, A. (2024). How 'European sovereignty' became mainstream: The geopoliticisation of the EU's'sovereign turn' by pro-EU executive actors. *Journal of European Integration*, *46*, 545–565. https://doi.org/10.1080/07036337.2024.2326831
Russell, A. L. (2014). *Open Standards and the Digital Age*. Cambridge University Press.
Schipper, F., & Schot, J. (2011). Infrastructural europeanism, or the project of building Europe on infrastructures: An introduction. *History and Technology*, *27*(3), 245–264. https://doi.org/10.1080/07341512.2011.604166
Schmidt, V. A. (2013). Democracy and legitimacy in the European union revisited: Input, output and 'throughput'. *Political Studies*, *61*(1), 2–22. https://doi.org/10.1111/j.1467-9248.2012.00962.x
Susi, M., Benedek, W., Fischer-Lessiak, G., Kettemann, M., Schippers, B., & Viljanen, J. (2022). *Governing information flows during war: A comparative study of content governance and media policy responses after Russia's attack on Ukraine*. Preprint/Working Paper Verlag Hans-Bredow-Institut. https://doi.org/10.21241/ssoar.78580
Ververis, V., Lasota, L., Ermakova, T., & Fabian, B. (2023). Website blocking in the European union: Network interference from the perspective of open Internet. *Policy & Internet*, *16*, 121–148. https://doi.org/10.1002/poi3.367
Zajácz, R. (2019). *Reluctant power: Networks, corporations, and the struggle for global governance in the early 20th century*. MIT Press.

SUPPORTING INFORMATION

Additional supporting information can be found online in the Supporting Information section at the end of this article.

How to cite this article: ten Oever, N., Perarnaud, C., Kristoff, J., Müller, M., Resing, M., Filasto, A., & Kanich, C. (2024). Sanctions and infrastructural ideologies: Assessing the material shaping of EU digital sovereignty in response to the war in Ukraine. *Policy & Internet*, 1–19. https://doi.org/10.1002/poi3.422

19442866, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1002/poi3.422 by University Of Illinois, Wiley Online Library on [13/09/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License