SIDN Labs

https://sidnlabs.nl

February 29, 2024

Author Version

Title: Internet Sanctions on Russian Media: Actions and Effects

Authors: John Kristoff, Moritz Müller, Arturo Filastò, Max Resing, Chris Kanich and Niels ten Oever

Published in: Free and Open Communications on the Internet

Link to original: https://www.petsymposium.org/foci/2024/foci-2024-0001.php

Internet Sanctions on Russian Media: Actions and Effects

John Kristoff
University of Illinois Chicago
jkrist3@uic.edu

Moritz Müller
SIDN Labs and University of Twente
moritz.muller@sidn.nl

Arturo Filastò
OONI
arturo@ooni.org

Max Resing
University of Twente
m.resing-1@student.utwente.nl

Chris Kanich
University of Illinois Chicago
ckanich@uic.edu

Niels ten Oever
University of Amsterdam
mail@nielstenoever.net

ABSTRACT

As a response to the Russian aggression against Ukraine, the European Union (EU), through the notion of 'digital sovereignty,' imposed sanctions on organizations and individuals affiliated with the Russian Federation that prohibit broadcasting content, including online distribution. In this paper, we interrogate the implementation of these sanctions and interpret them as a means to translate the union of states' governmental edicts into effective technical countermeasures. Through longitudinal traffic analysis, we construct an understanding of how ISPs in different EU countries attempted to enforce these sanctions, and compare these implementations to similar measures in other western countries. We find a wide variation of blocking coverage, both internationally and within individual member states. We draw the conclusion that digital sovereignty through sanctions in the EU has a concrete but distinctly limited impact on information flows.

KEYWORDS

sanctions, filtering, censorship, Russia

1 INTRODUCTION

In response to the Russian aggression against Ukraine, in 2022 the European Union instated sanctions against "media outlets under the permanent direct or indirect control of the leadership of the Russian Federation" to "introduce further restrictive measures to suspend the broadcasting activities of such media outlets in the Union, or directed at the Union."

These sanctions are a novel form of government-initiated network manipulation in several ways: unlike enforcement efforts aimed at e.g. torrent or streaming sites, the domain names were not seized; unlike traditional national censorship mechanisms (e.g. China's), the blocking is being done by a collection of sovereign nations, and is targeted at a specific, finite set of outlets rather than aiming to be a comprehensive information control mechanism.

Perhaps most importantly, this effort is not being centrally coordinated by an individual sovereign entity, but rather by many countries, each engaging with the internet companies within their own purview. This event presents an opportunity to investigate a federated, governmental approach to restricting the flow of internet traffic. We combine several vantage points and analyses of several different approaches to internet sanctions to perform a multidimensional characterization of these actions and their impacts.

This paper makes the following contributions:

(1) We contribute the first measurement study characterizing internet sanctions carried out by a closely coordinating collection of states, namely the European Union.
(2) We find that the most widespread sanction mechanism is DNS blocking (rather than seizures), and the most complete blocking is performed nearest the destination, but that blocking itself is far from uniform or ubiquitous, and that circumvention via techniques like mirroring is not successfully policed.
(3) Synthesizing these results, we conclude that while at a governmental level the EU was effectively able to coordinate its policy posture with respect to sanctioning these entities, the union has not been able to coordinate the technical implementation of these sanctions to largely or fully block access. While these sanctions no doubt introduced a measurable reduction in traffic to the sanctioned entities, complete or near-total blockage of sanctioned entities will require new, closer forms of coordination at the organizational or technical level.

2 BACKGROUND

Transnational communication networks have traditionally been used by nation states to exert power outside of their territory, while preventing other nation states from doing so in return [64]. To gain control over information networks, states use different strategies. Some do so by engaging in the governance of the internet [7], such as standard-setting [56] [18] or policy making around critical internet resources [8] [38]. However, in these arenas states need to contend with other actors. In response, several states have made policy proposals to enhance their 'digital sovereignty' [14] or 'data sovereignty' [28, 39]. Attempts to limit routes nationally or regionally have thus far largely failed [19], but filtering of information is a commonly used approach [17].

States regularly engage in the unilateral censoring of information on the internet, and do so in a variety of technical means [26]. Another way of providing instructions for network operators and infrastructure providers to engage in censorship is through multilateral internet sanctions. Some would argue that both forms of censorship have contributed to permanent internet fragmentation, which not only complicates technical operations, but necessitates the need for greater international cooperation.[22] In their overview

Free and Open Communications on the Internet (1), 1–12

paper Drake et al [20] describe three kinds of internet fragmentation: commercial, technical, and governmental. internet sanctions interestingly transverse all these categories.

2.1 International sanctions

In the international arena, a sanction is instantiated by a country in response to the doing of another country. There are different kinds of sanctions, that range from military actions and sporting events, to diplomatic and economic sanctions. Here we will focus on economic sanctions. In economic sanctions a country limits transactions, the provision of services, or travel by citizens of a particular country, or particular actors (such as a subsection of the inhabitants of a target country). In the past sanctions have been placed on telecommunications equipment as a tool in trade wars [27, 52]. However, sanctions have not just targeted networking equipment, but also traffic flows. An early example of this was documented in a recent report [1] that described a case as early as 1999, when a satellite internet connection provider from the United States wondered whether it would be in violation of sanctions against Yugoslavia if it would provide services there. This very early case clearly stipulates an inherent risk of sanctions, namely an over-compliance and disproportionate effect on general populations and therefore their impact on human rights [48], which is problematic because sanctions are regularly invoked in response to human rights violations [33]. To address this countries often seek to provide carve-outs in sanctions to create more targeted sanctions that do not negatively impact large populations [25]. However, these carve-outs do not always have the desired effect because of over-compliance by the companies that need to implement these sanctions against particular actors. Furthermore, companies regularly keep measures they have taken due to sanctions in place after the sanctions have been lifted, thus again leading to over-compliance [5].

2.2 Russia/Ukraine war and EU sanctions

The current and ongoing aggression against Ukraine started with the annexation of Crimea and illegal military operations in Ukraine's eastern Donbas region by the Russian states in February 2014. In February 2022 Russia started a full scale invasion attempt of Ukraine.

The EU has introduced sanctions against Russia since 2014. The first round of EU sanctions were announced in March 2014 and primarily consisted of travel sanctions. The second round of sanctions in April 2014 were expanded and the EU made it explicit that sanctions were not aimed at harming people, but designed to bring about change in behavior. In a third round, more entities and persons were added to the EU sanctions against Russia which added up to a total of 151 individuals and 37 entities. By February 2022, sanctions were applied to Russian oil and gas, the banking sector, as well as the technology and weapons industries. These are the heaviest sanctions ever adopted by the EU.

What is most notable from the most recent sanctions is that in March 2022 the EU banned the broadcasting of the news outlets Sputnik and RT. On June 2 2022, the media outlets Rossiya RTR/RTR Planeta, Rossiya 24 and TV Center International were added as well as the clarification that Russian state-controlled stations and channels are barred from distributing their content across the EU, whether via cable, satellite, internet, or smartphone apps. Furthermore, advertising products or services on these stations or channels was also forbidden.

2.3 Research scope

This paper is exclusively focused on characterizing the impact of the sanctions passed by the EU on the internet communication of the sanctioned media entities, its mechanisms, dynamics, and overall success. While there have been concrete requests by the government of Ukraine to internet governance and infrastructure actors ICANN and RIPE, these fall outside of the remit of this paper. The same is holds true for initiatives such as the Internet Sanctions Project [62], that seeks to provide guidance for the implementation of internet sanctions for network operators, and thereby bridging the gap between policy makers and implementers and limiting over-compliance. This article will also not focus on the provisioning of numbering and addressing resources to sanctioned actors, such as those provided by RIPE NCC, the Regional Internet Registry, which is registered in the Netherlands (and thus falls under EU law) that covers Europe, the former Soviet Union, and the Gulf region.

2.4 Ethics

As with many Internet measurement experiments, intentional consideration of ethical ramifications of the work are of the utmost concern. We utilized existing network measurement platforms that ensure active tests are run from systems designed for such purpose and minimize opportunities for abuse. Measurement platforms that utilized vantage points not under our sole administrative control have informed consent procedures in place and enforce firm restrictions on experiments that may be conducted. However, we raised three unique areas of potential concern not explicitly covered elsewhere.[15, 29]

(1) Our active measurements may raise sanctions enforcement alarms on systems we do not control.
(2) Our active measurements may expose noncompliance with a network's sanctions enforcement expectations.
(3) Our active measurement traffic may be unwelcome on the infrastructure of a country at war.

Given that our experiments were of modest type, duration, and scope, and that we only attempt to make limited contact to potentially sanctioned resources, we believe that our study poses no risk on the first concern. To address concern two we do not highlight any specific networks that may be obligated, but fail to comply with necessary sanctions enforcement requirements. We also do not publish the source IP address of the vantage points used in any active measurements. Regarding the final concern, in addition to carefully construed low-impact active measurement tests, we avoid the use of RIPE Atlas probes and EduVPN exit points located within Ukraine to limit the amount of traffic we place on that country's infrastructure.

Our research study was reviewed by two separate institution review boards, one in Europe and another in the United States. They both concurred with our analysis and approved the experiments.

3 METHODOLOGY & DATA

In this section we provide a high-level overview of our experiments, measurement methodologies, and collected data. Our aim is to understand how access to select Russian resources may have been affected due to sanctions enforcement. We focus on connectivity and access to Russian media organizations from vantage points in Europe unless otherwise noted. We do not examine nor collect any traffic except that which is generated or required by own active measurements through the platforms RIPE Atlas, EduVPN, Dataplane.org and NLNOG RING or provided by OONI. All active measurements, including those originating from within Ukraine are designed to be low-impact and nonrecurring. For our RIPE Atlas measurements, we send 12 DNS queries per domain name spread over a period of three hours. OONI data is retrieved from the public s3 bucket and the raw data is reprocessed using the OONI Data tool[45]. OONI measurements are collected through their global network of volunteers who have gone through an informed consent procedure where they are informed of the risks associated with participating in this active measurement collection [47]. EduVPN, Dataplane.org, and NLNOG RING measurements are manual nonrecurring and each vantage point (VP) is accessed sequentially with each measurement run in serial to prevent measurement traffic synchronization toward targets.

3.1 Sanctioned resource selection

Block lists of domain names, IP addresses, URLs, or routing information are commonly used to enforce network operator policies. In early 2022 we considered two technical proposals that use block list techniques to enforce internet sanctions against Russia. One is an ambitious, community cooperative project focused on transparency. [62] Another is a DNS-based firewall approach that blocks access to IP addresses geo-located to any country under sanction by the US government. [35]. We found no evidence that either approach has been widely deployed, nor consensus how they should be deployed.

We then evaluated US and European economic sanction lists published by national and regional government agencies. One of the best known and most influential is from The Office of Foreign Assets Control (OFAC) in the US Department of Treasury (USDOT). OFAC maintains and enforces economic sanctions targeting various entities around the globe, but it is primarily a list of foreign agencies, commercial organizations, and individuals. [41] This list data is populated with names, aliases, and known physical addresses, but may also include associated internet resources such as as URLs, email addresses, or cryptocurrency wallet identifiers. However, we often found the internet-specific attributes in OFAC data to be incomplete, inconsistent, or inaccurate. Furthermore, we could find no evidence that the OFAC list was being widely used for internet sanctions enforcement. EU-based sanctions regulations were more scattered as shown in Table 3 in Appendix A. In many of these sanctions data sets, we found similar issues that would make transforming them into internet block list solutions difficult.

Despite the apparent consistency and specificity challenges with existing economic sanctions data, multilateral internet sanctions against Russia began to take shape immediately following the February 24, 2022 attacks on Kyiv. Implementation details from network providers were few and far between with some ISPs grudgingly left to work out the details for themselves.[58] We decided to construct our own list drawn from multiple authoritative sources. See Table 3. The focus on Russian media in our study reflects the focus of sanctions from official European governing bodies, but we also include two well-known Russian banks and a branch of the Russian government that have been sanctioned by the US. In most of our experiments we also utilize two *control* web sites that are not covered by any known sanctions. One is a static, benign web site on a U.S. academic network. The other is the `icanhazip` IP address test site run by Cloudflare. [36]

3.2 Experiments and measurements

Internet sanctions enforcement may occur at a variety of points in the communications path or at different layers in a protocol stack. To evaluate enforcement we examine access across four broad dimensions: reachability, Domain Name System (DNS) response, Transport Layer Security (TLS) handshake, and Hypertext Transfer Protocol (HTTP) connection.

IP and transport reachability. We issue a series of ICMP, TCP, and UDP traceroute probes to our sanctions list to identify when enforcement occurs at the IP or transport layers. Traceroute access failures typically indicate network-layer enforcement mechanisms such as a packet filter on a firewall or via a firewalls or black hole route announcement. Where applicable, failures above the IP layer by experiments described below are also recorded.

DNS query response behavior. For each domain in our sanctions list we perform both A and AAAA DNS queries over UDP transport. Few names have associated AAAA (IPv6) address mappings and we are limited by each vantage point's local network configuration whether we can conduct experiments over both IPv4 and IPv6. Unless otherwise indicated, all results are based on IPv4 transport. When necessary, we perform identification queries to detect the resolver configuration if it is not directly available to us.

We identify block-attempts by relying on fingerprints published by OONI [44]. Additionally, we manually examine if IP addresses point towards websites. If the website contains information about blocking efforts, we classify the response as a block-attempt. Finally, we classify DNS responses containing errors or non-routable IP addresses (like 127.0.0.1) as block-attempts.

TLS handshake. We perform a TLS handshake to the IP addresses associated with port 443 on the targets and perform TLS certificate verification. We can detect TLS MiTM attempts by evaluating whether the server X.509 certificate returned is valid given the SNI and destination IP address in our requests when validated against the Mozilla root certificate list[37].

HTTP*S* request. Once a TLS session has been established we attempt to retrieve the content of the homepage by issuing a HTTP GET request for the / resource. We issue requests over both HTTP (80) and HTTPS (443) where applicable. For each session we record all relevant HTTP response meta data (e.g., headers and response status code) as well as body content.

3.3 Network measurement platforms

For our study we rely on a variety of network measurement platforms, summarized in Table 1. Combined, these platforms allow

Table 1: Measurement platforms and supported connectivity tests.

Platform	IP/TCP	DNS	TLS	HTTP(S)
OONI	TCP only	✓	✓	HTTPS only
RIPE Atlas	✗	✓	✗	✗
EduVPN	✓	✓	✗	✓
Dataplane.org	✓	✗	✗	✓
NLNOG RING	✓	✗	✗	✓

us to run and evaluate a variety of network experiments from in-country vantage points. The OONI and RIPE Atlas platforms are widely used, well understood, and described elsewhere.[23, 55] In OONI most URLs were already part of the testing lists and those missing were added in April 2023[54]. EduVPN, Dataplane.org, and the NLNOG RING may be less familiar to readers so we briefly summarize them below.

EduVPN is a federated VPN project coordinated by SURFnet, the National Research & Education Network (NREN) for the Netherlands. [21] Participating organizations can provide two types of access: *Institute Access* and *Secure Internet*. The former grants access to the internal resources of the host institution. The latter, which we use, only grants access to the public internet through a trusted server. Our motivation for using EduVPN is to assess the enforcement of sanctions in academic and research networks. We setup individual VPN connections at each EduVPN server to appear as a local client on the host network. DNS resolution configuration varies by institution. We had access to 11 academic networks, of which four were within the EU.

Dataplane.org is a non-profit network observation and measurement platform that operates over 300 dedicated and virtual Linux server systems. [16] The majority of vantage points are in hosting provider data centers around the globe. While these systems may not reflect end-user experiences, they help provide additional insight into sanctions enforcement seen in hosting environments or at the country-level. Almost all vantage points on this platform utilize Google Public DNS.[24]

NLNOG RING is project administered by the non-profit Netherlands Network Operator Group (NLNOG).[40] This platform is a collaborative troubleshooting network consisting of over 600 Linux-based virtual machines (VMs) in many distinct autonomous systems around the world. Participating networks contribute VMs and in return are granted access to all others in the network. The platform is widely used by network operators to troubleshoot and debug network-related issues using common Unix-based tools. All vantage points use a locally installed DNS resolver.

4 RESULTS

4.1 A view from OONI Probes

Since we care to know how sanctions enforcement is implemented (via DNS, TCP/IP, or TLS) we first determine if the DNS responses are consistent. Given an IP address and domain name pair, we consider an answer to be DNS consistent if it is possible to successfully establish a TLS handshake using the domain in the SNI from any vantage point [57]. If we don't do this first, we might misinterpret the TLS failure as a signal for TLS-level blocking rather than via the DNS.

For addresses which are not DNS consistent, we manually determine if they are serving block pages. We include a sample of block pages in Appendix A. If the DNS is consistent, we proceed to the TCP connection and TLS handshake. For each of these, we consider a failure to be an indication of blocking and categorize them based on the specific error condition.

In order to assess the impact of the sanctions from all country origins, we are interested in understanding how many ISPs in each country are blocking which sites. Since DNS-based blocking is very prevalent in Europe[59], we introduce an additional disaggregation based on the configured resolver of the OONI Probes. We refer to a resolver configuration as "Internal Resolver", when the probe's IP address and resolver IP address are both originated from the same ASN. Otherwise the resolver is labeled "External Resolver", which indicates the resolver service is provided by an upstream ISP or third-party DNS provider.

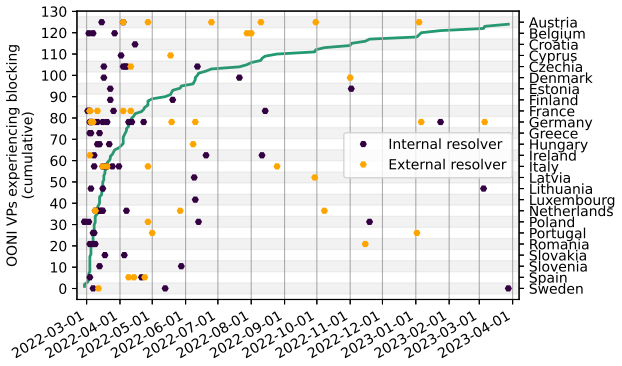

Figure 1: Longitudinal view of first-seen blocking of www.rt.com as observed by OONI. The dark-green is the total number of ASes for which blocking has been observed. 77% of these ASes enforce sanctions within 3 months.

In the vast majority of cases an external resolver that performs blocking is a larger regional upstream ISP. Since sanctions enforcement on most public DNS resolver providers is rare, this also allows us to learn how many networks would allow sanctions enforcement to be trivially circumvented by merely switching the resolver to an alternative service. We plot the longitudinal results in Figure 1.

In Figure 2 we illustrate the frequency of enforcement mechanism types used for `www.rt.com`, which is the domain where blocking is most common and for which we have the most measurements. The error codes are defined in the OONI df-007-errors specification. [46] Some additional code are created through some custom analysis. Specifically we mark as `dns.confirmed` when we see an answer pointing to a known blockpage based on fingerprints in [43], `dns.bogon` indicates an answer contains a bogon IP address, while `tls.bad_cert` consolidates all the TLS related errors code starting with `ssl_`.

Table 2: Percentage 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	33	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	37	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	37	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	92	99	100	97	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

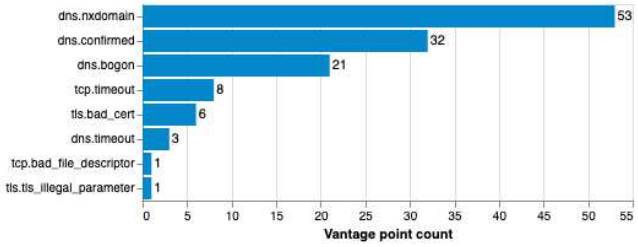

Figure 2: Methods used by ISPs in Europe to implement filtering (OONI Data)

4.2 DNS according to RIPE Atlas

Table 2 summarizes the measurement results between 2022-08-01 and 2023-09-19 per country and domain name. Each cell shows the share of responses that were not blocked.

For each country, we select all available probes and query for the A record of each domain name using the probe's recursive resolver. To increase measurement reliability, we only rely on probes that run on software version 3 or higher. Also, we do not show results if we collected responses from two VPs or less.

Table 2 also shows that there is some form of DNS blocking in all countries in the European Union (EU). At the same time, however, our measurements show the extent to which blocking occurs differs widely. For example, while VPs in Slovenia experience frequent blocking for domain names in the first round, no VP experiences blocking for domain names belonging to organizations added in the later rounds. In comparison, VPs in France also experience blocking for most domain names added later to the sanctions list, however not as often as the initial list of domain names. We found practically no evidence of DNS-based blocking of US-sanctioned Russian banks or government domains. Outside of the EU, we find some evidence of blocking on the small number of media outlets sanctioned by the UK government.

Interestingly, the block lists and their implementation in member countries and Internet Service Providers (ISPs) were inconsistent over time. For example, the German regulator removed two domain names from their list after their operators removed sanctioned content[6]. Our measurements show that over-compliance varied as not all ISPs stopped blocking the corresponding domain names

right away, but after a few months the sites became reachable by all ISPs again.

In contrast, the ISPs in Austria started blocking certain domains only after a few months, even though they were specified months in advance and already blocked in Germany. Furthermore, as an example of under-compliance, the newly registered and sanctioned name for Sputniknews, `sputnikglobe.com` has not yet been widely blocked as of this writing.

Overall, DNS-based blocking is present, but varies from provider to provider. Domain names that belong to organizations listed in the first Council of the European Union decision [11] are blocked more often than domain names added later. 45% of our VPs received at least one blocked response for domain names related to organizations were listed in the first package (i.e., version of the sanctions list). This number decreases with each new round of packages: from 19% in the second to 17% in the fourth round.

4.3 Lessons From EduVPN networks

Arguably, the users of academic and research networks have a high expectation, desire, and need for open and unrestricted access to information. Internet sanctions however may be at odds with certain academic pursuits. Therefore, we also want to evaluate if sanctions enforcement is present on these networks as well.

We configured 11 measurement Virtual Machines (VMs) to connect to each of the available networks supporting the EduVPN platform. Each VM tunneled traffic through its connected EduVPN session to a tunnel gateway using the DNS resolvers provided by the VPN session. We validated the DNS responses using Google's public DNS service. The tests were run on May 09, 2023.

Four of the EduPVN networks fall under the legislation of the EU. These are located in *Germany, Denmark, Finland*, and *the Netherlands*. Each of these networks announce a DNS resolver in their own IP address space. Our results focus on these four institutions. The non-European EduVPN sites show little evidence of sanctions enforcement.

We observed different results in all four European research networks. The Danish institution exhibited a limited amount of blocking. All domain names were resolved as expected. We only observed failed TCP and HTTP/HTTPS tests on the mirror sites of Sputnik News.

In contrast, a Finish institution exhibited the most complete blocking with negative TCP and web responses for most news outlets and corresponding mirror sites. DNS responses however were positive and valid.

The German and a Dutch institutions were similar to one another, revealing that most media domains were unreachable via TCP and HTTP/HTTPS. However, the behavior of the DNS between these networks differs slightly. In the German network, the resolvers return `NXDOMAIN` responses, while the Dutch network answers with `SERVFAIL`. We summarize results in Figure 3.

4.4 Hosting environments and sanctions

Reachability and HTTP(s) measurements run through Dataplane.org and NLNOG RING platforms are conducted in a fashion similar to those performed in the EduVPN environment described above. We ran HTTP/HTTPS and network connectivity tests on three

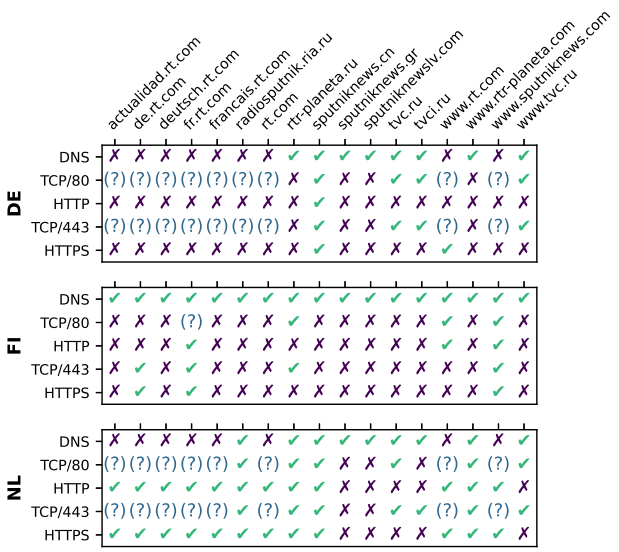

Figure 3: Measurement observations of three EduVPN institutions. Measurements marked with a "?" indicate the default limit of 30 hops was exceeded.

separate occasions in May 2023. We verified all VPs were able to reach at least one of our two control targets. Our tests include retry mechanisms to smooth over any natural, short-lived effects of host, path, and destination variants given the size and diversity of VPs.

The results from both Dataplane.org and NLNOG RING are similar, but NLNOG RING VPs were noticeably less reliable and exhibited greater inconsistency. Both platforms show high high levels of blocking to `sputniknewstv.com` throughout the EU region. However, while Dataplane.org VPs exhibited no serious problems accessing HTTPS at our control nodes, a number of NLNOG RING VPs would occasionally fail. We believe a larger proportion of the Dataplane.org VPs fared better due to comparatively smaller average load, greater available resources, and better than average environmental stability.

The use of Google DNS on the Dataplane.org platform and local resolver on NLNOG RING result in relatively few instances of DNS-based sanctions enforcement. Therefore, we focus on reachability and HTTP(S) connection tests.

Figure 4 summarizes the success rate of HTTPS reachability to our sanction list from the Dataplane.org vantage points. Overall blocking is relatively modest, largely due to the use of Google DNS, but we find interesting anomalies when we scan the table vertically. For example, at the time of measurements, `sputniknews.gr` and `sputniknewslv.com` were both hosted by a popular DDoS mitigation provider used by many Russian networks. These domains were largely inaccessible from most of the EU. We manually verified that traffic between many countries and those sites is being blocked. A similar situation appears to have occurred with `www.gazprombank.ru`, which was listed in the USDOT OFAC sanctions list. We don't know the motivation, but these DDoS mitigation providers appear to have been performing sanctions enforcement

based on IP access control from countries that imposed sanctions. It is also worth nothing that these blocks do not show up in our DNS-based measurements.

5 DISCUSSION

5.1 Transparency of blocking

When analysing our measurements, we noticed network providers convey vastly different messages to their users when access to a sanctioned internet resource has been blocked, if they communicate a reason at all,

Overall, the vast majority of ISPs choose to implement blocking by some form of DNS-based filtering. RIPE Atlas measurements §4.2 suggest 50% of ISPs return a DNS error response to queries requesting a blocked domain name and in three VPs feedback is conveyed via Extended DNS Errors [31] (info code 15 - blocked). OONI measurements §4.1 show that 87% of the 125 VPs implementing blocks chose to do so via DNS. Of these, only 32 serve a block page, meaning that in 74% of cases where blocking is implemented the user is not informed of the reason why the resource is inaccessible.

The usefulness of block pages also varies. Some inform users the domain name is blocked because of Russia sanctions (e.g. Figure 5). Others only show a generic block page that are also used for sites blocked due to copyright infringement (e.g. Figure 6).

5.2 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 (RT) (see Table 3). In Germany, those domain names were listed on correspondence by the regulator with groups representing the local internet industry [6]. Additionally, the Austrian provider Liwest published the Spanish domain names on their block page [32].

Table 2 shows that in the majority of countries these new mirror pages are not always blocked. For example, the Spanish sites are only blocked by Austrian providers, but not in Spain as we would have expected. On the other hand, German mirror pages are blocked by most providers in Austria and in 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. A possible explanation could be a load-balancer that forwards queries to resolvers with diverging block lists but we could not confirm this theory.

We found another exception with the domain name `rtde.live`. This domain is blocked in Austria but not in Germany whereas the third level domain names `test.rtde.live` is only blocked in Germany. This is in accordance with the sanctions by the German regulator, which lists `test.rtde.live` but not its second level variant.

The list provided by the German regulator also contains domain names not directly related to the sanctioned organizations, but which facilitate the distribution of their content. These include websites that allow visitors to stream the channels of RT among others. These names change with some regularity and we can use these changes to observe correlated sanctions enforcement changes. For example, we saw that after the German regulator removed the domain names `www.russisches-tv-fernsehen.de` and `www.coolstreaming.us` from the block list German ISPs followed suite accordingly. Our measurements from August 2022 show that German networks that originally blocked these domain names have lifted the blocks again.

5.3 Implementation of sanctions in NRENs

As already mentioned in section 4.3, researchers and academics have a keen desire to access otherwise restricted information. Therefore, we wondered if research facilities would be excluded from the regulations. Our work provides evidence that some NRENs adhere to sanctions enforcement. The measurements of a Finnish NREN reveal a rather broad implementation of sanctions. Our observation of the German and Dutch networks align with DNS-based enforcement of regular German ISPs. Only a research network in Denmark appears to be less strict in comparison to national ISPs. A comparison of Table 2 and Figure 3 support these findings.

5.4 Placement of enforcement mechanisms

We found DNS-based blocking was the dominant form of implementing internet sanctions. Functionally however, networks vary widely in how DNS-based blocking was performed. Some networks redirect users to a page that may or may not explain why a resource was blocked. Others simply return DNS errors, sometimes with extended error codes, but usually not. Many networks rely on third party resolution service such as Google Public DNS or Cloudflare DNS, which do not appear to implement any sanctions enforcement regardless of location. As long as a user can utilize an alternative DNS resolver, they would be able to bypass most sanctions enforcement.

We found some evidence of IP address access control to enforce sanctions. These mechanisms were typically the most complete and successful because they were applied close to or at the destination where the restricted content was hosted. While this approach was most effective, it was also the the least popular type of mechanism deployed. This approach would also pose the greatest risk of "over-blocking" when multiple systems and services share an IP address, which may explain why it was rarely employed.

6 RELATED WORK

The Russian invasion in the Ukraine and immediate consequences on internet connectivity has sparked the interest of the research community. In addition to generally network availability issues, internet censorship was studied in the context of the war of Ukraine. However, to the best of our knowledge, no studies focus on internet sanctions within the EU. The OONI project team has measured censorship within Russia and show that censorship was extended to a broader set of sites and services in the course of the conflict [53, 63]. Also Ramesh et al. show that censorship on Russian users increased. [51]. Additionally, they study the use of a new domestic certificate authority and the use and blocking of censorship circumvention tools.

Other literature and reports focused on the response of services and infrastructure in the Ukraine and in Russia. Jonker et al. [30] study how the infrastructure of Russian websites and DNS infrastructure changed in the course of the conflict. Luconi et al. study the impact on routing and latency in the Ukraine [34].

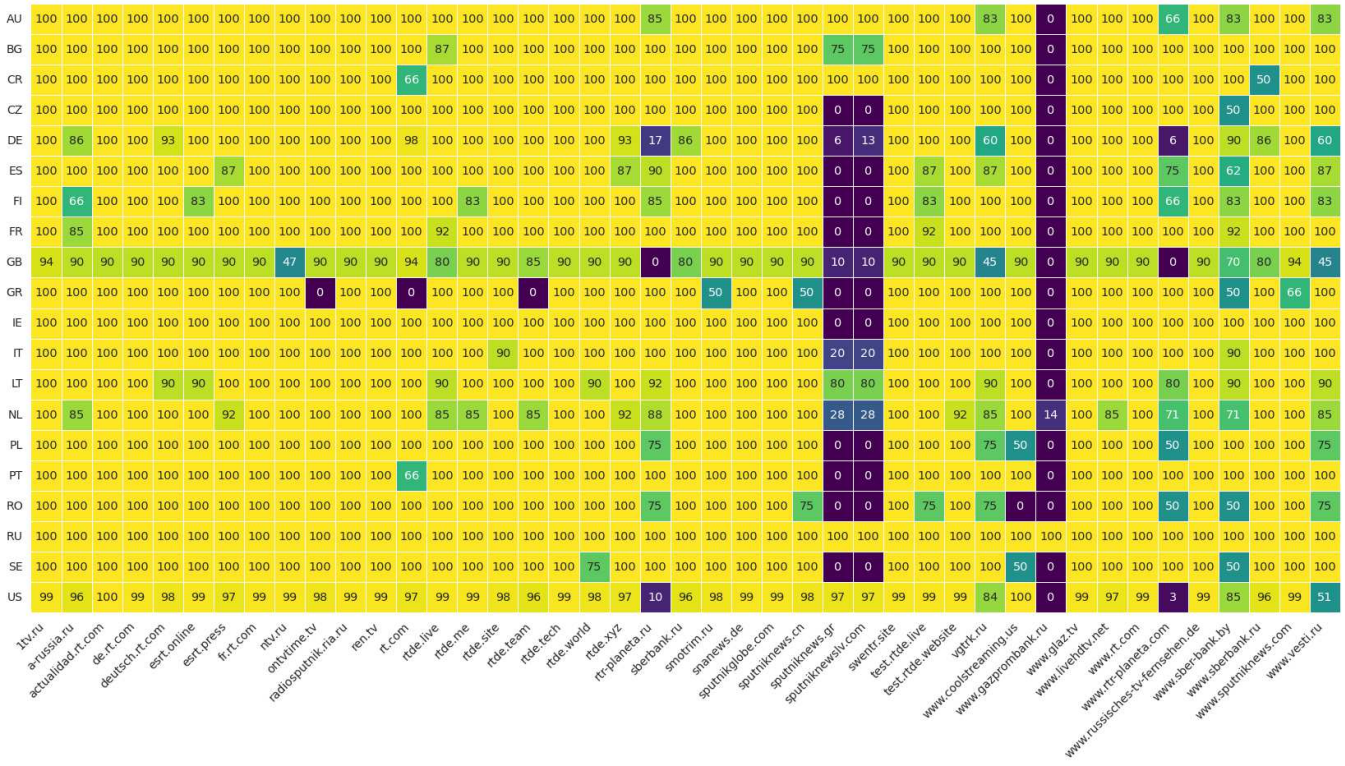

Figure 4: HTTPS reachability success rate (2xx or 3xx HTTP response status code) from Dataplane.org VPs.

Outside of the scope of the Russian invasion, online censorship has been studied extensively. Poort et al. study censorship and impact in Europe in the context of copyright infringement [50]. Their focus was on ISPs in the Netherlands and not on the technical implementation of the measures. Bortzmeyer has used RIPE Atlas probes to measure censorship worldwide [3]. There, he also discusses caveats when using RIPE Atlas probes to measure censorship. Ververis et al. study the impact of censorship in mobile app stores [60]. The work of Ververis et al. [61] comes close to our own. Using OONI they consider censorship generally, examining block list consistency and web censorship behavior throughout EU member countries.

Finally, the topic of digital sovereignty has also gained traction in the social science community. Perarnaud et al. analyse various EU policies on digital sovereignty and their impacts [49]. Braud et al. and Baur et al. both analysed digital sovereignty by looking at the "European Cloud" project Gaia-X [2, 4]. With our analysis we add a novel perspective on the issue of digital sovereignty in the EU and for the future of internet sanctions.

7 CONCLUSIONS

In this article we have analyzed how EU sanctions against Russian media, in response to the Russian aggression in Ukraine, have been implemented. What we have found is that these sanctions are inconsistently implemented across the EU. The inconsistent implementation of the sanctions can at least in part be attributed to the high-level description of the sanctions and the lack of recommendations for technical implementation. This left implementation of the sanctions largely to the interpretation of network operators without sufficient guidance provided by national authorities in EU member states. This led to a diffuse implementation and thus it could be argued has had limited impact to increasing the EU's digital sovereignty. However, it could be also be said that this is typical for EU policy making, which always involves raised tensions when it comes to the sovereignty of individual member states.

While the sanctions might not have proven to be as efficient and effective as some may have liked, we anticipate this is just an early harbinger into a new era of multilateral internet sanction events. This may also accelerate the discursive concept of digital sovereignty into a technical reality. Future work could compare the implementation of sanctions with other approaches to attain digital sovereignty, specifically in the EU due to its supranational nature and inherent tension between governance layers.

REFERENCES

[1] Farzaneh Badiei. 2023. *Sanctions and the Internet.* Technical Report. Digital Meduda, RIPE NCC, Amsterdam. https://digitalmedusa.org/wp-content/uploads/2023/05/SanctionsandtheInternet-DigitalMedusa.pdf

[2] Andreas Baur. 2023. European Dreams of the Cloud: Imagining Innovation and Political Control. *Geopolitics* (2023), 1–25. Publisher: Taylor & Francis.

[3] Stéphane Bortzmeyer. 2015. DNS Censorship (DNS Lies) As Seen By RIPE Atlas. *RIPE Labs* (2015). https://labs.ripe.net/author/stephane_bortzmeyer/dns-censorship-dns-lies-as-seen-by-ripe-atlas/

[4] Arnaud Braud, Gaël Fromentoux, Benoit Radier, and Olivier Le Grand. 2021. The Road to European Digital Sovereignty with Gaia-X and IDSA. *IEEE Network* 35, 2 (March 2021), 4–5. https://doi.org/10.1109/MNET.2021.9387709 Conference

Name: IEEE Network.
[5] Emmanuel Breen. 2021. Corporations and US economic sanctions: the dangers of overcompliance. In *Research Handbook on Unilateral and Extraterritorial Sanctions*. Edward Elgar Publishing, 256–269. https://www.elgaronline.com/display/edcoll/9781839107849/9781839107849.00024.xml Section: Research Handbook on Unilateral and Extraterritorial Sanctions.
[6] Bundesnetzagentur. accessed 2023. Sanktionslisten, Sperrlisten und Overblocking. https://fragdenstaat.de/anfrage/sanktionslisten-sperrlisten-und-overblocking/.
[7] Madeline Carr. 2015. Power Plays in Global Internet Governance. *Millennium* 43, 2 (Jan. 2015), 640–659. https://doi.org/10.1177/0305829814562655
[8] George Christou and Seamus Simpson. 2007. Gaining a stake in global internet governance: The EU, ICANN and strategic norm manipulation. *European journal of communication* 22, 2 (2007), 147–164. Publisher: Sage Publications Sage UK: London, England.
[9] Council of the European Union. 2022. Council Decision (CFSP) 2022/2478 of 16 December 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022D2478.
[10] Council of the European Union. 2022. Council Decision (CFSP) 2022/327 of 25 February 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukrainee. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022D0327.
[11] 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022D0351.
[12] Council of the European Union. 2022. Council Decision (CFSP) 2022/884 of 3 June 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022D0884.
[13] Council of the European Union. 2023. Council Decision (CFSP) 2023/434 of 25 February 2023 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022D2478.
[14] Stephane Couture and Sophie Toupin. 2019. What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society* 21, 10 (Oct. 2019), 2305–2322. https://doi.org/10.1177/1461444819865984 Publisher: SAGE Publications.
[15] Jedidiah R Crandall, Masashi Crete-Nishihata, and Jeffrey Knockel. 2015. Forgive Us our SYNs: Technical and Ethical Considerations for Measuring Internet Filtering.. In *NS Ethics@ SIGCOMM*. 3.
[16] Dataplane.org. [n. d.]. https://dataplane.org.
[17] R. J. Deibert, J. G. Palfrey, R. Rohozinski, and J. Zittrain (Eds.). 2008. *Access Denied: The Practice and Policy of Global Internet Filtering*. MIT Press, Cambridge, MA.
[18] Laura DeNardis. 2014. *The Global War for Internet Governance*. Yale University Press, New Haven.
[19] Daniel Dönni, Guilherme Sperb Machado, Christos Tsiaras, and Burkhard Stiller. 2015. Schengen Routing: A Compliance Analysis. In *Intelligent Mechanisms for Network Configuration and Security (Lecture Notes in Computer Science)*, Steven Latré, Marinos Charalambides, Jérôme François, Corinna Schmitt, and Burkhard Stiller (Eds.). Springer International Publishing, 100–112.
[20] William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter. 2016. *Internet Fragmentation: An Overview*. Technical Report. World Economic Forum, Cologny, Canton of Geneva, Switzerland. https://www.weforum.org/reports/internet-fragmentation-an-overview
[21] EduVPN. [n. d.]. https://www.eduvpn.org.
[22] Nathaniel Fick, Jami Miscik, Adam Segal, and Gordon M. Goldstein. 2022. *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*. Technical Report. Council on Foreign Relations. https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace
[23] Arturo Filastò and Jacob Appelbaum. 2012. OONI: Open Observatory of Network Interference. In *2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI 12)*. USENIX Association, Bellevue, WA. https://www.usenix.org/conference/foci12/workshop-program/presentation/Filast{ò}
[24] Google Public DNS. [n. d.]. https://developers.google.com/speed/public-dns/.
[25] Jerg Gutmann, Matthias Neuenkirch, and Florian Neumeier. 2020. Precision-guided or blunt? The effects of US economic sanctions on human rights. *Public Choice* 185, 1-2 (2020), 161–182. Publisher: Springer.
[26] Joseph Lorenzo Hall, Michael D. Aaron, Amelia Andersdotter, Ben Jones, Nick Feamster, and Mallory Knodel. 2023. *A Survey of Worldwide Censorship Techniques*. Internet Draft draft-irtf-pearg-censorship-10. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-irtf-pearg-censorship Num Pages: 45.
[27] Yu Hong. 2017. *Networking China: The Digital Transformation of the Chinese Economy* (illustrated edition ed.). University of Illinois Press, Urbana, Chicago, and Springfield.
[28] Patrik Hummel, Matthias Braun, Max Tretter, and Peter Dabrock. 2021. Data sovereignty: A review. *Big Data & Society* 8, 1 (Jan. 2021), 2053951720982012. https://doi.org/10.1177/2053951720982012 Publisher: SAGE Publications Ltd.
[29] Ben Jones, Roya Ensafi, Nick Feamster, Vern Paxson, and Nick Weaver. 2015. Ethical concerns for censorship measurement. In *Proceedings of the 2015 ACM SIGCOMM Workshop on Ethics in Networked Systems Research*. 17–19.
[30] Jonker, Mattijs and Akiwate, Gautam and Affinito, Antonia and Claffy, kc and Botta, Alessio and Voelker, Geoffrey M and van Rijswijk-Deij, Roland and Savage, Stefan. 2022. Where .ru? Assessing the Impact of Conflict on Russian Domain Infrastructure. In *Proceedings of the 22nd ACM Internet Measurement Conference*. 159–165.
[31] W. Kumari, E. Hunt, R. Arends, W. Hardaker, and D. Lawrence. 2020. Extended DNS Errors. RFC 8914 (Proposed Standard). https://doi.org/10.17487/RFC8914
[32] Liwest. accessed 2023. Netzsperren Liwest. http://86.56.128.186/.
[33] George A. Lopez and David Cortright. 1997. Economic Sanctions and human rights: part of the problem or part of the solution? *The International Journal of Human Rights* 1, 2 (1997), 1–25. Publisher: Taylor & Francis.
[34] Valerio Luconi and Alessio Vecchio. 2023. Impact of the first months of war on routing and latency in Ukraine. *Computer Networks* 224 (2023), 109596. https://doi.org/10.1016/j.comnet.2023.109596
[35] MacFarlane, Druce. 2022. Infoblox Response to Ukraine Crisis. https://blogs.infoblox.com/security/infoblox-response-to-ukraine-crisis.
[36] Major Hayden. 2021. A aew future for icanhazip. https://major.io/2021/06/06/a-new-future-for-icanhazip.
[37] Mozilla. [n. d.]. https://wiki.mozilla.org/CA.
[38] Milton Mueller. 2010. *Networks and states: The global politics of Internet governance*. MIT press.
[39] Milton Mueller. 2017. *Will the Internet fragment?: sovereignty, globalization and cyberspace*. OCLC: 962233256.
[40] NLNOG RING. [n. d.]. https://ring.nlnog.net.
[41] Office of Foregin Assets Control, U.S. Department of the Treasury. [n. d.]. https://ofac.treasury.gov/ofac-sanctions-lists.
[42] Office of Foreign Assets Control. 2023. Specially Designated Nationals and Blocked Persons list. https://sanctionssearch.ofac.treas.gov/Details.aspx?id=35845. Accessed: May 26, 2023.
[43] OONI Blocking Fingerprints. [n. d.]. https://github.com/ooni/blocking-fingerprints/.
[44] OONI blocking-fingerprints [Online]. [n. d.]. https://github.com/ooni/blocking-fingerprints/blob/main/fingerprints_dns.csv.
[45] OONI Data Kraken. [n. d.]. https://github.com/ooni/data.
[46] OONI Spec DF007 Errors. [n. d.]. https://github.com/ooni/spec/blob/master/data-formats/df-007-errors.md.
[47] Open Observatory of Network Inteference (OONI). [n. d.]. https://ooni.org/about/risks.
[48] Dursun Peksen. 2009. Better or worse? The effect of economic sanctions on human rights. *Journal of Peace Research* 46, 1 (2009), 59–77. Publisher: Sage Publications Sage UK: London, England.
[49] Clément Perarnaud, Julien Rossi, Francesca Musiani, and Lucien Castex. 2022. *'Splinternets': Addressing the renewed debate on internet fragmentation*. Technical Report PE 729.530. European Parliamentary Research Service, Brussels. 80 pages. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729530/EPRS_STU(2022)729530_EN.pdf
[50] Joost Poort, Jorna Leenheer, Jeroen van der Ham, and Cosmin Dumitru. 2014. Baywatch: Two approaches to measure the effects of blocking access to The Pirate Bay. *Telecommunications Policy* 38, 4 (2014), 383–392.
[51] Reethika Ramesh, Ram Sundara Raman, Apurva Virkud, Alexandra Dirksen, Armin Huremagic, David Fifield Dirk Rodenburg, Rod Hynes, Doug Madory, and Roya Ensafi. 2022. Network Responses to Russia's Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom. (2022).
[52] Svetlana Viktorovna Rimkevich and Yuri Anatolievich Savinov. 2019. Economic sanctions as a trade war tool in telecom equipment market. *Russian Foreign Economic Journal* 7 (2019), 75–89. https://ideas.repec.org//a/alq/rufejo/rfej_2019_07_75-89.html Publisher: Russian Foreign Trade Academy Ministry of economic development of the Russian Federation.
[53] Roskomsvoboda. 2022. How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine. *OONI* (2022). https://ooni.org/post/2023-russia-a-year-after-the-conflict/
[54] Russian media github pull request. [n. d.]. https://github.com/citizenlab/test-lists/pull/1271.
[55] RIPE Ncc Staff. 2015. Ripe atlas: A global internet measurement network. *Internet Protocol Journal* 18, 3 (2015), 2–26.
[56] Niels ten Oever and Stefania Milan. 2022. The Making of International Communication Standards: Towards a Theory of Power in Standardization. *Journal of Standardisation* 1 (June 2022). https://doi.org/10.18757/jos.2022.6205
[57] Elisa Tsai, Deepak Kumar, Ram Sundara Raman, Gavin Li, Yael Eiger, and Roya Ensafi. 2023. CERTainty: Detecting DNS Manipulation at Scale using TLS Certificates. *Proceedings on Privacy Enhancing Technologies* 2023, 3 (jul 2023), 122–137. https://doi.org/10.56553/popets-2023-0073
[58] UK sanctions law, A&A, and Domain blocking. [n. d.]. https://www.aa.net.uk/etc/news/uk-sanctions-law-aa-and-domain-blocking/.

[59] Vasilis Ververis, Tatiana Ermakova, Marios Isaakidis, Simone Basso, Benjamin Fabian, and Stefania Milan. 2021. Understanding Internet Censorship in Europe: The Case of Spain. In *13th ACM Web Science Conference 2021*. 319–328.
[60] Vasilis Ververis, Marios Isaakidis, Valentin Weber, and Benjamin Fabian. 2019. Shedding Light on Mobile App Store Censorship. In *Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization (UMAP'19 Adjunct)*. Association for Computing Machinery, New York, NY, USA, 193–198. https://doi.org/10.1145/3314183.3324965
[61] Vasilis Ververis, Lucas Lasota, Tatiana Ermakova, and Benjamin Fabian. 2023. Website blocking in the European Union: Network interference from the perspective of Open Internet. *Policy & Internet* (2023).
[62] We, The Undersigned. 2022. Multistakeholder Imposition of Internet Sanctions. https://wiki.sanctions.net/index.php/The_Open_Letter.
[63] Maria Xynou and Arturo Filastò. 2022. New blocks emerge in Russia amid war in Ukraine: An OONI network measurement analysis. *OONI* (2022). https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/
[64] Rita Zajácz. 2019. *Reluctant Power: Networks, Corporations, and the Struggle for Global Governance in the Early 20th Century*. MIT Press.

A BLOCK PAGES, TIMELINE, SANCTIONS LIST

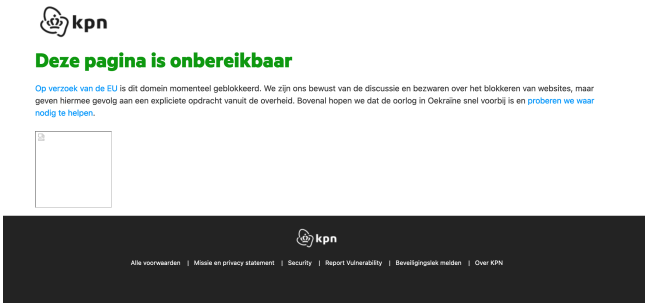

Figure 5: Blocking page of a Dutch ISP. The text states "Upon the request of the EU [link to the Dutch version of [11]], this domain is currently blocked. We are aware of the discussion and objections about blocking websites, but we are complying with an explicit order from the government. Above all, we hope that the war in Ukraine will soon be over and we will try to help where needed." (translated by the authors).

Figure 6: Blocking page of a Portuguese ISP. The text states "The contents you are trying to access are blocked and are protected by Copyright and Related Rights. Its access, use and/or disclosure, without the authorization of the respective holder, is a crime provided for and punished by law." (translated by Google Translate).

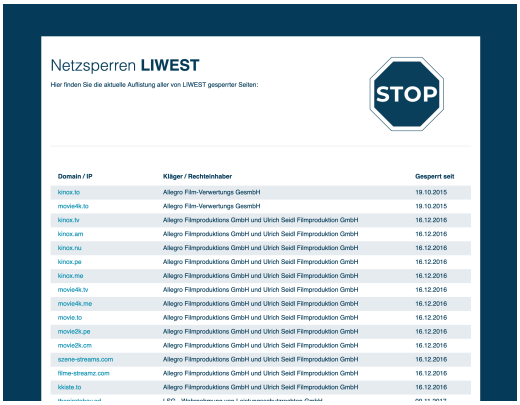

Figure 7: Blocking page of an Austrian ISP. The page lists all currently blocked pages, the entity requesting the block, and the date the block was added.

Blocked on	Country	Probe ASN	DNS ASN	
2022-02-27	Poland	5617	5617	dns.nxdomain
		6830	6830	dns.bogon
2022-03-02	France	5410	5410	dns.nxdomain
2022-03-03	Belgium	6848	6848	dns.confirmed
	France	3215	3215	dns.bogon
		12322	12322	dns.bogon
	Poland	12741	12741	dns.nxdomain
2022-03-04	France	2200	36692	tcp.timeout
		8228	15557	dns.nxdomain
		15557	15557	dns.nxdomain
	Germany	3320	3320	dns.nxdomain
	Greece	3329	3329	dns.nxdomain
	Ireland	15751	5466	dns.confirmed
	Romania	8708	8708	dns.confirmed
	Spain	57269	57269	dns.bogon
2022-03-05	Germany	3209	3209	dns.nxdomain
		3320	0	dns.nxdomain
		8767	8767	dns.nxdomain
		8881	8881	dns.nxdomain
	Greece	6799	6799	dns.bogon
	Lithuania	25406	25406	dns.nxdomain
2022-03-07	Belgium	5432	5432	dns.confirmed
	Germany	198967	64666	dns.nxdomain
	Portugal	3243	3243	dns.confirmed
	Romania	12302	12302	dns.nxdomain
	Sweden	2119	2119	dns.timeout
2022-03-08	Germany	6805	6805	dns.nxdomain
	Ireland	6830	6830	dns.confirmed
	Italy	29447	29447	dns.bogon
	Portugal	2860	2860	dns.bogon
2022-03-09	Netherlands	1136	8737	dns.confirmed
		206238	64666	tls.bad_cert
			206238	dns.timeout
	Romania	9050	9050	dns.bogon
2022-03-11	France	15557	64666	dns.nxdomain
	Germany	8422	8422	dns.nxdomain
	Hungary	20845	20845	dns.nxdomain
	Netherlands	33915	33915	dns.confirmed
2022-03-12	Sweden	39651	1257	dns.bogon
2022-03-13	Greece	5408	5408	dns.timeout
	Hungary	5483	5483	dns.bogon
	Netherlands	1136	1136	dns.confirmed
	Slovenia	34779	34779	dns.nxdomain
2022-03-15	Austria	8412	8412	dns.confirmed
	Netherlands	13127	13127	dns.confirmed
2022-03-16	Germany	20676	20676	dns.nxdomain
	Italy	3269	3269	dns.bogon
		21333	15169	tcp.timeout
	Lithuania	8764	8764	dns.bogon
	Netherlands	50266	50266	dns.confirmed
2022-03-17	Czechia	13036	13036	dns.nxdomain
	Denmark	197288	197288	dns.confirmed
	Italy	35612	35612	dns.nxdomain
2022-03-18	Italy	12874	12874	dns.bogon
	Netherlands	33915	6830	dns.confirmed
	Slovakia	5578	5578	dns.confirmed
2022-03-19	Italy	1267	1267	dns.nxdomain
2022-03-20	Germany	198967	198967	dns.nxdomain
	Italy	30722	30722	dns.nxdomain
			64666	dns.nxdomain
2022-03-22	Hungary	21334	21334	dns.nxdomain
2022-03-23	Estonia	2586	2586	dns.confirmed
	Finland	719	719	dns.nxdomain
2022-03-25	Italy	8612	8612	dns.nxdomain
2022-03-26	France	2200	2200	tcp.timeout
2022-03-27	Belgium	47377	47377	dns.bogon
2022-03-31	Italy	16232	16232	dns.bogon

Figure 8: Timeline of blocking of www.rt.com across providers in Europe

Blocked on	Country	Probe ASN	DNS ASN	
2022-04-02	Cyprus	35432	35432	tls.bad_cert
2022-04-04	Austria	1901	8447	dns.nxdomain
		8447	8447	dns.nxdomain
	Czechia	5610	5610	dns.nxdomain
	France	3215	0	dns.bogon
2022-04-05	Slovakia	6855	6855	dns.bogon
2022-04-06	Czechia	50698	50698	dns.confirmed
2022-04-07	Czechia	21430	21430	dns.nxdomain
	Netherlands	1103	1103	dns.nxdomain
2022-04-09	Germany	62336	62336	dns.nxdomain
	Spain	6739	12430	tls.bad_cert
2022-04-11	Czechia	21430	64666	dns.nxdomain
	France	51207	12322	dns.bogon
2022-04-12	Germany	12693	12693	dns.timeout
2022-04-14	Spain	12430	15169	tls.bad_cert
2022-04-15	Croatia	5391	5391	dns.bogon
2022-04-21	Spain	3352	3352	dns.nxdomain
2022-04-23	Germany	9145	9145	dns.nxdomain
2022-04-24	Spain	205836	15169	tls.bad_cert
2022-04-27	Austria	51265	13335	dns.confirmed
	Italy	21333	36692	tcp.timeout
	Poland	43939	12741	dns.nxdomain
2022-05-01	Portugal	12353	15169	dns.nxdomain
2022-05-13	Sweden	3301	3301	dns.confirmed
2022-05-18	Cyprus	6866	36692	dns.confirmed
2022-05-19	Germany	8422	64666	dns.nxdomain
2022-05-20	Finland	1759	1759	dns.confirmed
2022-05-27	Netherlands	15703	15169	tcp.timeout
2022-05-28	Slovenia	3212	3212	dns.nxdomain
2022-06-08	Hungary	21334	15169	tcp.timeout
2022-06-09	Latvia	24921	24921	dns.confirmed
2022-06-10	Germany	8881	20880	dns.nxdomain
	Luxembourg	8632	8632	dns.confirmed
2022-06-12	Czechia	16019	16019	dns.nxdomain
2022-06-13	Poland	12912	12912	dns.nxdomain
2022-06-20	Ireland	2110	2110	dns.nxdomain
2022-06-25	Austria	40980	47147	dns.nxdomain
2022-07-21	Denmark	44034	44034	dns.confirmed
2022-07-28	Belgium	5432	13335	dns.confirmed
2022-08-01	Belgium	5432	15169	dns.confirmed
2022-08-10	Austria	12793	8447	dns.nxdomain
2022-08-11	Ireland	5466	5466	tcp.timeout
2022-08-14	France	52075	52075	dns.bogon
2022-08-25	Italy	210278	5607	tls.illegal_param..
2022-09-29	Latvia	24921	12847	dns.confirmed
2022-09-30	Austria	8559	8339	dns.confirmed
2022-10-08	Netherlands	33915	13335	tcp.timeout
2022-11-01	Denmark	197288	39642	dns.confirmed
2022-11-02	Estonia	3249	3249	dns.nxdomain
2022-11-15	Romania	35725	9050	dns.bogon
2022-11-19	Poland	39603	39603	dns.confirmed
2023-01-02	Portugal	42863	3243	dns.confirmed
2023-01-04	Austria	51265	15169	dns.confirmed
2023-01-06	Germany	59790	59790	dns.nxdomain
2023-01-24	Germany	51978	51978	dns.nxdomain
2023-03-05	Lithuania	39007	39007	dns.nxdomain
2023-03-06	Germany	3320	35487	tcp.bad_file_des..
2023-03-28	Sweden	1257	1257	dns.nxdomain

Figure 9: Timeline of blocking of www.rt.com across providers in Europe

Table 3: Sanctioned organisation, measured hostnames, and source.

Sanctioned organisation	Hostname	Source	Remark/Date added
Russia Today English	www.rt.com	Council Decision 2022/351 [11]	1 March 2022
Russia Today UK	www.rt.com	Council Decision 2022/351 [11]	1 March 2022
Russia Today Germany	de.rt.com	Council Decision 2022/351 [11]	1 March 2022
	deutsch.rt.com	Council Decision 2022/351 [11]	1 March 2022
Russia Today France	francais.rt.com	Council Decision 2022/351 [11]	1 March 2022
	fr.rt.com	Council Decision 2022/351 [11]	1 March 2022
RT en español	actualidad.rt.com	Council Decision 2022/351 [11]	1 March 2022
	actualidad-rt.com	Council Decision 2022/351 [11]	1 March 2022
Sputnik	www.sputniknews.com	Council Decision 2022/351 [11]	1 March 2022
	sputniknewslv.com	Council Decision 2022/351 [11]	1 March 2022
	sputniknews.gr	Council Decision 2022/351 [11]	1 March 2022
	sputniknews.cn	Council Decision 2022/351 [11]	1 March 2022
	radiosputnik.ria.ru	Council Decision 2022/351 [11]	1 March 2022
	sputnikglobe.com	Council Decision 2022/351 [11]	Registered 29 March 2023, sputniknews.com now redirects to this domain name.
Rossiya RTR / RTR Planeta	www.rtr-planeta.com	Council Decision 2022/884 [12]	3 June 2022
	rtr-planeta.ru	Council Decision 2022/884 [12]	3 June 2022
	vgtrk.ru	Council Decision 2022/884 [12]	3 June 2022
Rossiya 24 / Russia 24	www.vesti.ru	Council Decision 2022/884 [12]	3 June 2022
TV Centre International	www.tvc.ru	Council Decision 2022/884 [12]	3 June 2022
	tvci.ru	Council Decision 2022/884 [12]	3 June 2022
NTV/NTV Mir	ntv.ru	Council Decision 2022/2478 [9]	16 December 2022
Rossiya 1	smotrim.ru	Council Decision 2022/2478 [9]	16 December 2022
REN TV	ren.tv	Council Decision 2022/2478 [9]	16 December 2022
Pervyi Kanal	1tv.ru	Council Decision 2022/2478 [9]	16 December 2022
RT Arabic	www.rtarabic.com	Council Decision 2023/434 [13]	25 February 2023
Sputnik Arabic	sputnikarabic.ae	Council Decision 2023/434 [13]	25 February 2023
RT en español mirror	esrt.online	Liwest Blocklist [32]	Registered 8 April 2022
	esrt.press	Liwest Blocklist [32]	Registered 8 April 2022
RT Germany mirror	rtde.site	Bundesnetzagentur [6]	Registered 5 March 2022
	rtde.xyz	Bundesnetzagentur [6]	Registered 5 March 2022
	rtde.team	Bundesnetzagentur [6]	Registered 5 March 2022
	test.rtde.live	Bundesnetzagentur [6]	Registered 6 April 2022
	rtde.live	Bundesnetzagentur [6]	Registered 6 April 2022
	test.rtde.website	Bundesnetzagentur [6]	Registered 6 April 2022
	rtde.tech	Liwest Blocklist [32]	Registered 6 April 2022
	rtde.world	Liwest Blocklist [32]	Registered 6 April 2022
	rtde.me	Liwest Blocklist [32]	Registered 6 April 2022
A-Russia	a-russia.ru	Bundesnetzagentur [6]	Russian TV streaming site
WWITV: World Wide Internet TV	wwitv.com	Bundesnetzagentur [6]	TV streaming site
glaz.tv	www.glaz.tv	Bundesnetzagentur [6]	TV streaming site
Russisches Fernsehen	www.russisches-tv-fernsehen.de	Bundesnetzagentur [6]	TV streaming site
On TV Time	ontvtime.tv	Bundesnetzagentur [6]	TV streaming site
SPB TV World	spbtv.online	Bundesnetzagentur [6]	TV streaming site
Coolstreaming	www.coolstreaming.us	Bundesnetzagentur [6]	TV streaming site
Live HD TV	www.livehdtv.net	Bundesnetzagentur [6]	TV streaming site
Rossiya Segodnya Group	snanews.de	Liwest Blocklist [32]	German news site
State Duma	duma.gov.ru	OFAC Sanctions list [42]	
Sberbank	www.sber-bank.by	Council Decision 2022/327 [10]	25 February 2022, Not part of Annex IX
	www.sberbank.ru	Council Decision 2022/327 [10]	25 February 2022, Not part of Annex IX
Gazprombank	www.gazprombank.ru	Council Decision 2022/2478 [9]	16 December 2022, Not part of Annex IX