Received: 28 March 2023 | Accepted: 13 August 2023

DOI: 10.1002/poi3.367

RESEARCH ARTICLE

P&I Policy & Internet PSO WILEY

Website blocking in the European Union: Network interference from the perspective of Open Internet

Vasilis Ververis[1,2,3] | **Lucas Lasota**[1] | **Tatiana Ermakova**[4] | **Benjamin Fabian**[5]

[1]Humboldt-Universität zu Berlin, Berlin, Germany

[2]Weizenbaum Institute for the Networked Society, Berlin, Germany

[3]Critical Infrastructure Lab, Department of Media, University of Amsterdam, Amsterdam, The Netherlands

[4]Hochschule fü r Technik und Wirtschaft (HTW) Berlin, Berlin, Germany

[5]Technical University of Applied Sciences Wildau (TH Wildau), Wildau, Germany

Correspondence

Vasilis Ververis, Humboldt-Universität zu Berlin, Berlin, Germany.
Email: ververis@kth.se

Abstract

By establishing an infrastructure for monitoring and blocking networks in accordance with European Union (EU) law on preventive measures against the spread of information, EU member states have also made it easier to block websites and services and monitor information. While relevant studies have documented Internet censorship in non-European countries, as well as the use of such infrastructures for political reasons, this study examines network interference practices such as website blocking against the backdrop of an almost complete lack of EU-related research. Specifically, it performs and demonstrates an analysis for the total of 27 EU countries based on three different sources. They include first, tens of millions of historical network measurements collected in 2020 by Open Observatory of Network Interference volunteers from around the world; second, the publicly available blocking lists used by EU member states; and third, the reports issued by network regulators in each country from May 2020 to April 2021. Our results show that authorities issue multiple types of blocklists. Internet Service Providers limit access to different types and categories of websites and services. Such resources are sometimes blocked for unknown reasons and not included in any of the publicly available blocklists. The study concludes with the hurdles related to network measurements and the nontransparency

from regulators regarding specifying website addresses in blocking activities.

KEYWORDS

blocklist, DNS manipulation, EU, Internet censorship, national regulation authority, network interference, Open Internet, website blocking

INTRODUCTION

In setting up the infrastructure for monitoring and network blocking to adhere to the EU legislation for preventive dissemination measures of terrorist content, gambling regulations, copyright enforcement, tobacco and health website regulations, extremism, phishing, and hate speech (Angelopoulos, 2009; Zittrain & Palfrey, 2007), EU member states have made it easier to block websites and services and to monitor information. Here, Internet Service Providers (ISPs) and network operators are (often) required to set up blocking infrastructures. Permitted practices concerning traffic management that can involve filtering by ISPs are regulated at the first stage by the Open Internet Regulation (EU) 2015/2120 (Council of the European Union, 2015). In respect to Open Internet principles, network traffic interference practices such as blocking, slowing down, altering, restricting, degrading or discriminating between specific content, applications, services, or specific categories of content, applications, or services are not in principle allowed. They are subject to justified and narrowly defined exceptions in the law. Article 3(3) of the Open Internet Regulation sets the framework for such activities in the EU. In this regard, the European regulator BEREC has provided guidelines for the implementation of the Open Internet Regulation that have laid down the exceptions in which ISPs may implement such traffic management regulations (Council of the European Union, 2015). However, the evidence provided in this paper demonstrates a lack of transparency in the ways in which network interference is conducted in the EU countries. Although website blocking is a current activity, regulators have not provided enough evidence on how such blocking is being conducted by the telecommunication operators. EU member states not only use blocklists as a means of blocking access to websites but also block different types and categories of websites and services that are not included in the publicly available (identified) blocklists.

Relevant studies have documented Internet censorship in non-European countries, as well as usage of such infrastructures for other political motives (Shirazi & Greenaway, 2009; Poblet, 2018). We define Internet censorship as the practice of using any kind of hardware or software to prevent users from accessing websites or services through network interference or information control. In recent years, further studies have been conducted, which have drawn attention to online network interference and Internet blocking in individual countries of the EU (Aceto et al., 2016; Busch et al., 2018; Savola, 2015; Schmidt-Kessen et al., 2019; Ververis et al., 2015, 2017, 2021). For instance, the "Open Net Initiative" report mentions nearly 50 countries that practice Internet censorship (Aceto et al., 2016). To the best of the authors' knowledge, no analysis of network interference in all EU countries has been performed.

With regard to the blocking of websites as a current activity under insufficient documentation on how such blocking is carried out by the telecommunication operators, this research examines how network interference is conducted in the EU countries, to what extent EU member states use blocklists as a means of blocking access to websites and what different types and categories of websites and services are affected by these practices that are not included in the publicly accessible (identified) blocklists.

Contributions

This study provides three main contributions: The study contributes by conducting a comprehensive analysis of the 27 EU countries,[1] based on three different sources. These include, first, tens of millions of historical network measurements collected in 2020 by volunteers from around the world; second, the publicly available blocking lists used by EU member states; and third, all reports of all blocked websites issued by each country's network regulators.

The analysis of 27 EU countries is based on ten million historical network measurements collected during 2020 by Open Observatory of Network Interference (OONI) volunteers around the world (Open Observatory of Network Interference [OONI], 2020). OONI is an organization that develops software to perform network measurements. OONI also administers the server infrastructure to store these data in a database (see the OONI Backend section), from which data can be retrieved for further analysis, for instance, to identify cases of Internet censorship or to detect surveillance network equipment. Over the years, different types of methodologies have been developed to detect filtering or blocking of network resources, tampering with communication channels, and intentional manipulation of network routes. These types of blocking methodologies can be evaluated with network measurements: data contributed to OONI gathered by anonymous volunteers from each country who use software probes (OONI, 2020). These data depict a rigorous perspective of the actual network filtering or content blocking that occurs in a specific network. Network measurements are challenging to conduct as they are deployed from vantage points that either probes have access to, or are located within the underlying network being measured.

This research also lists and catalogs publicly available blocklists in the EU. The blocklists are used by EU member states to block access to websites or services. In the early 2000s, the EU issued regulations blocking access mainly to online gambling services that were not licensed by all EU member states. Contrary to other services, the EU has constrained online gambling operators to operate in each EU country by paying a licensing fee to each EU member state in which they provide online services. One of the ways to enforce this regulation was to issue website blocklists of the unlicensed gambling websites and oblige ISPs to censor them in their networks. This is one of the first instances of EU-wide website blocking that drove ISPs to create a filtering infrastructure in their networks, frequently with many inconsistencies, over-blocking, and under-blocking websites (Ververis et al., 2015). Lately, the censorship of websites has increased and more categories have been added to the blocklists ranging from streaming websites, subtitles, file sharing, and torrents to tobacco, health, and medicine information resources, as discussed in the Data analysis results section.

Finally, this paper reviews and provides a summary of the reports issued by the National Regulatory Authority (NRA) of each EU member state with information concerning network interference such as website blocking. Other institutions than the NRAs in each country may also regulate networks there.

Structure

The paper is structured as follows. First, after related research is described in the second section. The third section presents some essential foundations of this research, explaining the OONI architecture and network measurements in detail. The fourth section describes our methods for collecting and analyzing the network measurement data used in this study. The fifth section presents the results of our overall data analysis. We discuss current challenges, point out avenues for further research, derive practical implications, summarize our findings, and conclude in, the sixth section.

RELATED RESEARCH

Relevant research from previous academic studies has shown that censorship exists in many countries such as China (Chen et al., 2013; Clayton et al., 2006; Dunna et al., 2018; Ensafi et al., 2015; Holowczak & Houmansadr, 2015; Hounsel et al., 2018; King et al., 2013, 2014; Knockel et al., 2015, 2017, 2018; Lowe et al., 2007; Marczak et al., 2015; Ng et al., 2018; Park & Crandall, 2010; Robinson et al., 2013; Winter & Lindskog, 2012; Wright, 2012; Xu et al., 2011), Thailand (Gebhart et al., 2017), Bangladesh (Morshed et al., 2017), Pakistan (Aceto et al., 2016; Nabi, 2013), India (Gosain et al., 2017; Yadav et al., 2018), Iran (Anderson, 2012, 2013; Aryan et al., 2013), Syria (Al-Saqaf, 2016; Chaabane et al., 2014), Turkey (Tanash et al., 2015, 2017), Russia (Ramesh et al., 2020), and Mexico (Iszaevich, 2019). A few studies have looked at network interference and Internet blocking in the EU context (Busch et al., 2018; Savola, 2015; Schmidt-Kessen et al., 2019; Ververis et al., 2015, 2017, 2021). To the best of the authors' knowledge, there is no previous research analyzing network interference in all EU countries, specifically related to website blocking.

FOUNDATIONS: OONI ARCHITECTURE AND NETWORK MEASUREMENTS

OONI data are publicly released and provided as an open access data set, available under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International license (Filastò, 2018). OONI provides the blocking detection methodologies used by its software in the public domain for review, experimentation, and potential improvements by the community.

OONI software is released under a free license (GNU General Public License v3.0) and is publicly available for downloading, running, further distribution, modification, and improvement. Open methodologies build a capable and strong community of researchers, activists, policy advocates, hackers, data scientists, and others interested in researching Internet censorship. Having open methodologies and public access to the source code allows the community and volunteers to contribute to network measurements and make informed decisions about the potential privacy risks associated with the use of OONI software. In addition, such methodologies increase transparency regarding the validity of collected network measurements and allow a better understanding of the technical implementation and technical details of the lower level. A high-level diagram of the OONI infrastructure and software is shown in Figure 1.

The engine is the part of the software that runs the network measurements (nettests). OONI provides probes to perform the nettests. The probe software for mobile or desktop clients is based on different software implementations depending on the platform. Each probe (client) implementation uses a specific software architecture. The applications for mobile devices are

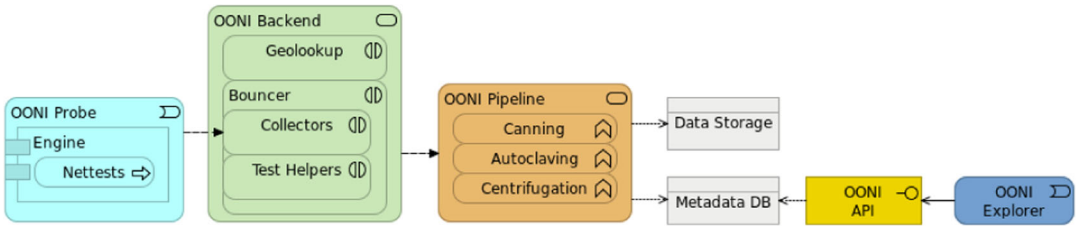

FIGURE 1 Open Observatory of Network Interference (OONI) high-level architecture diagram.

developed in Java for Android (probe-android) and Objective-C for iOS (probe-ios). The desktop clients are developed in Go for the command-line interface (probe-cli) and JavaScript for the desktop applications of MacOS, Windows, and Linux (probe-desktop). The legacy implementation (probe-legacy) for the desktop clients (still used despite its legacy status) is being developed in Python.

OONI backend

A typical transaction of an OONI probe to the backend consists of the following steps: (i) the probe requests the available collectors and test helpers from the bouncer; (ii) the probe performs a geolocation lookup to find out its IP address (deduced by default for privacy considerations) and determine the Autonomous System (AS) number, the country code, and the name of the network entity owning the AS; (iii) the probe opens a report for the nettest; (iv) upon completion of the nettest, the probe submits the results to the collector as a JSON file.

Once the results have been submitted, they are sent to the OONI pipeline for archiving and further processing of the network measurements (reports). The pipeline aggregates the data (reports) submitted by the probes (network measurement clients) to the backend. Upon receiving the unprocessed reports, the pipeline performs the following steps: (i) canning—compacts the reports to occupy less disk space and helps to reprocess the reports faster; (ii) autoclaving—sanitizes and normalizes the report data, removing potential personally identified information and fixing inconsistent data formats; (iii) centrifugation—aggregates the important parts of the reports and stores these metadata to a database for further processing.

Powered with data from the metadata database, the Application Programming Interface (API) allows analysis of data collected from OONI probes. This component is based on the Open API specification and is extensively documented. Finally, OONI Explorer (OONI Explorer—Open Data on Internet Censorship Worldwide, 2022) provides a visual representation of all OONI data and allows performing quick queries with various constraints such as (nettest, country, Uniform Resource Locator [URL], and date) in an easy and graphically visual way without the need to download any data or use the API.

OONI methodology

In our research, we analyze network measurement data performed by the Web Connectivity OONI nettest (OONI, 2019). This test measures the reachability and possible blocking of a website given an IP address or a domain name. The test's methodology diagram is illustrated in Figure 2. The Web Connectivity test consists of the following steps: (i) performing an A Domain Name System (DNS) lookup and storing the results of the A records list, (ii) attempting

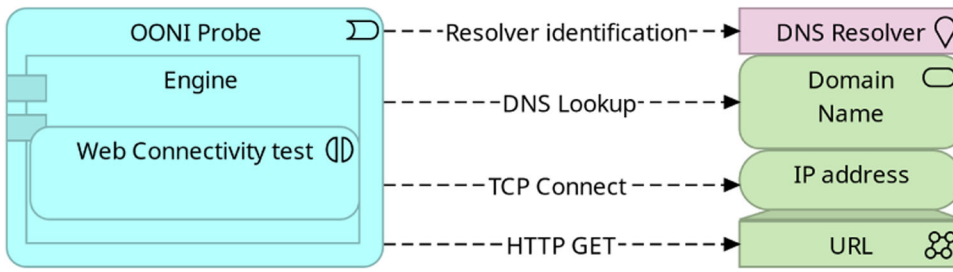

FIGURE 2 Open Observatory of Network Interference (OONI) Web Connectivity test diagram.

to establish a TCP session in either port 80 or 443 (depending on the URL scheme), (iii) performing an Hypertext Transfer Protocol (HTTP) GET request to the path specified in the Uniform Resource Identifier (URI). The responses and possible errors from each step are recorded in a JSON file and submitted to the OONI network measurements collector for further processing and archiving.

METHODS OF NETWORK ANALYSIS

In this study, we draw on historical OONI network measurement data. Using custom-built database queries, we were able to collect more than 10 million relevant network measurements. We then created a meta database (Filastò, 2019) in PostgreSQL to ease the workload of collecting, cleaning, and organizing our data set. We used the Jupyter Notebook software tool and the Python programming language to collect, process, clean, categorize, and analyze the OONI data. For the blocklists we performed web data scraping to extract the blocklists from the publication websites, Portable Document Format (PDF) files, and documents in other file formats, as the released blocklists are not systematically distributed. Moreover we conducted interviews and requested public blocklists and information related to the blocking of websites or services from multiple authorities via e-mail communication (see the Blocklists section for more details).

Criteria and distribution of data

In total, we analyzed almost one million unique network measurements (specifically 999,125) from 888 distinct ASes in 27 countries. The data distribution across networks and countries is not uniform. Some network measurements were submitted by volunteers at random intervals but many were submitted with consistent frequency. Figure 3 represents the distribution percentage of the analyzed network measurements per country. We use the Alpha-2 country code notation as described in the ISO 3166 international standard. Our data analysis criteria were the following: (i) network measurements present in the OONI meta database; (ii) data collected in the date range: 2020-01-01 to 2020-10-20; (iii) data flagged as anomalous (with signs of network interference); (iv) network measurements conducted from networks within the EU; (v) network measurements performed with the Web Connectivity test.

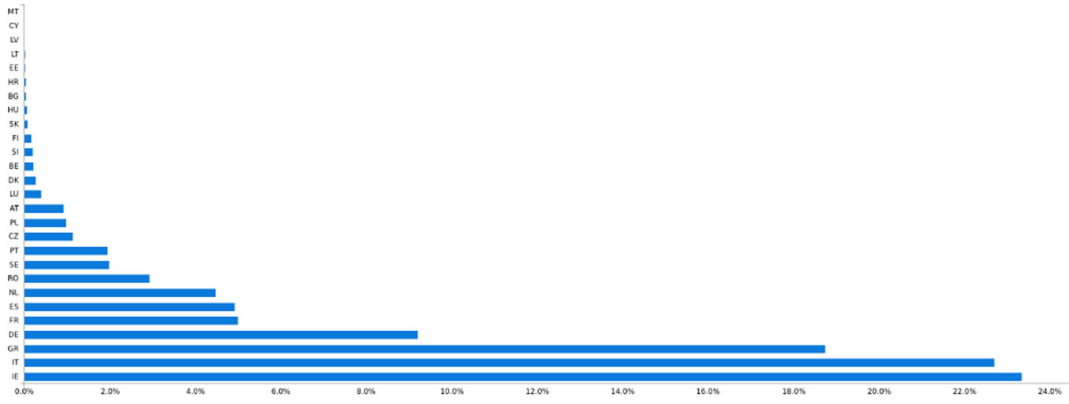

FIGURE 3 Data distribution per country code (Alpha-2 ISO 3166).

Data collection

To access the OONI data, we set up a PostgreSQL replica of the OONI meta database (Filastò, 2019) and we fetched the latest archived data required for a database cluster (Evdokimov, 2019). It took about 10 days to sync with the master database and required 800 GB of storage capacity to accommodate the OONI meta database. A helper script was used to fetch the OONI S3 bucket data and configure the PostgreSQL server as a replica (in a hot standby configuration). This script fetches the latest archived meta database replica instance using all the available CPUs for decompression. The main requirement of the replica is a system with enough storage capacity and network connectivity to host a PostgreSQL database. A description of the Web Connectivity OONI test methodology is provided in the OONI methodology section, and the test diagram is illustrated in Figure 2.

Data validation

We use the term blockpage to refer to an instance of deliberate blocking. The term has been, and sometimes also still is, used to refer to the error message displayed. From among the many network measurements with signs of network interference, we only included as blockpages those cases of which it could with some certainty be verified that they were neither false positives (for instance due to network connectivity errors) nor blocked due to internal network filtering rules (such as parental controls, antivirus filtering, or firewalls). For this, we derived a set of heuristics from certainly blocked instances and excluded all network measurements unless they satisfied the specified criteria: (i) existence of a blockpage or any indication of an error due to blocking (e.g., HTTP error codes); (ii) existence of DNS records that point to bogus IP addresses (such as 127.0.0.1); (iii) network measurements with correct AS information (i.e., if the probe's AS number is not shared, *AS0*).

Blockpage heuristics

Network measurements that present signs of network interference (anomalous data) are not always evidence of website blocking. In fact, it is quite common to find anomalies in network measurements due to transient network errors, website misconfigurations, geolocation blocking, or simply software issues and bugs. For this reason, we developed a number of heuristics to identify website blocking by manually looking into the data set, and verifying that is indeed a case of website blocking. We accept that website blocking has occurred when all the criteria set during the data validation process (see the Data validation section) are satisfied.

In addition to the data analysis criteria of Criteria and distribution of data section and the data validation criteria of the Data validation section, there is an additional test that a network measurement must satisfy for us to consider it to be a blockpage. On the validated data set we compare if the DNS A record of the website (IP address) is on the same AS as the one in the probe's network performing the measurement. This helps to detect the blockpages hosted within the same ISP or IP address ranges of the country. This is common and usual practice as it is unlikely that a website is hosted on the same AS as the one where the network measurement has been conducted.

National Regulatory Authorities' monitoring and reporting on Open Internet

As an obligation imposed by art. 5(1) of the Open Internet Regulation, the NRAs should annually inform the European Commission about their activities in monitoring and enforcing the Regulation's rules. The reports would serve as summaries for the Commission on the state of affairs in national jurisdictions and would serve to provide a minimum level of transparency and comparability of the implementations across Europe. Among the things expected to this end from the reports are the overall description of the national situation regarding network neutrality, the description of the NRAs' monitoring activities, the number and types of complaints, ISPs' infringements related to the Regulation, and results of surveys, evaluations, and technical measurements implemented by the NRAs. The reports from the NRAs should present any network blocking or network neutrality issue to the European commission based on the Open Internet regulation (Council of the European Union, 2015). We collected, analyzed and summarized all reports issued by each EU member state's NRA from May 2020 to April 2021. Table 1 summarizes each country's reports and refers to any blocking of websites or services mentioned in the annual reports of NRAs.

DATA ANALYSIS RESULTS

In our data analysis, we discovered several blocked websites in each country that were not listed in any public blocklist or mentioned in the annual Open Internet monitoring reports prepared by the NRA.

Our findings show a lack of transparency regarding network blocking in the EU countries. The data demonstrate that, although website blocking is a current activity, regulators have not provided enough evidence on how such blocking is being conducted by the telecommunication operators. This may result in over- or under-blocking websites, or network services being wrongfully blocked, as occurred in past incidents highlighted by some studies (Ververis et al., 2015, 2021).

Detected blockpages

We were able to identify 51 unique blockpages from 18 countries and 47 ASes that present a form of a blockpage or a generic error that is inconsistent with the network measurements of the control probe during the Web Connectivity test. Figure 4 illustrates all blockpages with the blockpage title per country code in the Alpha-2 ISO 3166 notation. Most countries present one or two blockpages while others present as many as seven. Such variation is due to network measurements performed nonuniformly by all countries, as we elaborate further in the Conclusion and further discussion section. Additionally, Figure 5 depicts all the categories of the blocked websites we detected in Figure 4, following the notation:

$$\{CountryCode - CategoryCode\}$$

The categories of the websites are extracted by Citizen Lab's URL test lists, the collaborative lists of websites or services curated and reviewed by community members to detect potentially blocked websites across countries (Citizen Lab et al., 2014). The details of the category description and code of each detected blockpage are listed in Table 2.

TABLE 1 National regulatory authorities reports overview.

Country	Report on blocking
Austria	Network blocking due to copyright law, Sec. 3.4 (part II) (Austrian Regulatory Authority for Broadcasting and Telecommunications, 2021)
Belgium	No cases of service or application blocking, Sec. 5.117 (Belgian Institute for Postal Services and Telecommunications, 2021)
Bulgaria	Blocking in accordance with national legislative acts, Sec. 1.2 (Communications Regulation Commission [CRC], 2021)
Croatia	None mentioned (HAKOM, 2021)
Cyprus	None mentioned (Cyprus Office of the Commissioner of Electronic Communications and Postal Regulation, 2021)
Czech Republic	None mentioned (Czech Telecommunication Office, 2021)
Denmark	42% of ISPs indicated they block access to Internet, Sec. 4.1 (Danish Energy Agency, 2021)
Estonia	None mentioned (Estonian Consumer Protection and Technical Regulatory Authority, 2021)
Finland	None mentioned (Niko et al., 2021)
France	None mentioned (Arcep, 2021)
Germany	An ISP blocked certain domains via DNS due to court ruling, Sec. 3.1.2 (Bundesnetzagentur, 2021)
Greece	Gambling and copyright blocklists, DNS and port blocking, Sec. 4.1.1 (National Telecommunications and Postal Commission, 2021)
Hungary	None mentioned (National Media and Communications Authority, 2021)
Ireland	Website blocking might be in place at a number of ISPs in April 2021, Sec. 27 (Commission for Communications Regulation, 2021)
Italy	None mentioned (AGCOM, 2021)
Latvia	None mentioned (The Public Utilities Commission, 2021)
Lithuania	None mentioned (Communications Regulatory Authority of the Republic of Lithuania, 2021)
Luxembourg	None mentioned (Luxembourg Institute of Regulation, 2021)
Malta	Ongoing investigation of IP blocking, Sec. 4 (Malta Communications Authority, 2021)
The Netherlands	None mentioned (Authority for Consumers & Markets, 2021)
Poland	Blocking traffic due to obligations under Article 15f(5) on gambling, and preventing access to websites using domain names published on the blocklist maintained by Cert Polska (Office of Electronic Communications, 2021)
Portugal	None mentioned (ANACOM, 2021)
Romania	ANCOM was given powers to issue decisions to block specific online content or websites presenting false news about COVID-19, and issued 15 blocking orders (The National Authority for Administration and Regulation in Communications [ANCOM], n.d), Sec. 1.1 (ANCOM, 2021)
Slovakia	ISPs block access based upon the European or national legislation; in the event of spreading illegal content, applications or services, or gambling websites without a Slovak license, were blocked, Sec. 2 (Slovak Republic Regulatory Authority for Electronic Communications and Postal Services, 2021)

(Continues)

TABLE 1 (Continued)

Country	Report on blocking
Slovenia	None mentioned (Slovenian Regulatory Authority for Electronic Communications and Postal Services, 2021)
Spain	Blocking of websites by request of the courts only, Sec. 3.2 (State Secretariat for Telecommunications, Digital Infrastructures of the Ministry of Economic Affairs, and Digital Transformation, 2021)
Sweden	None mentioned (Market Regulation Department Swedish Post and Telecom Authority, 2021)

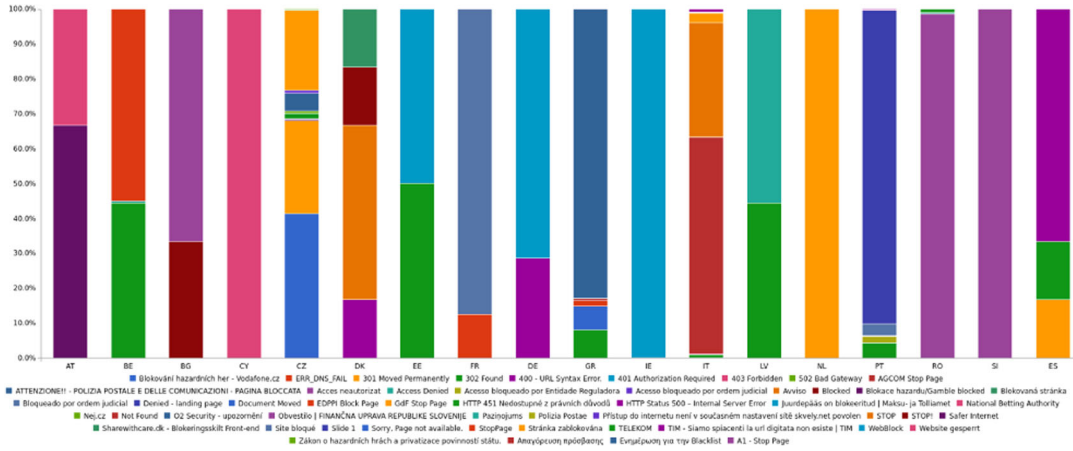

FIGURE 4 Blockpages per title and country code (Alpha-2 ISO3166).

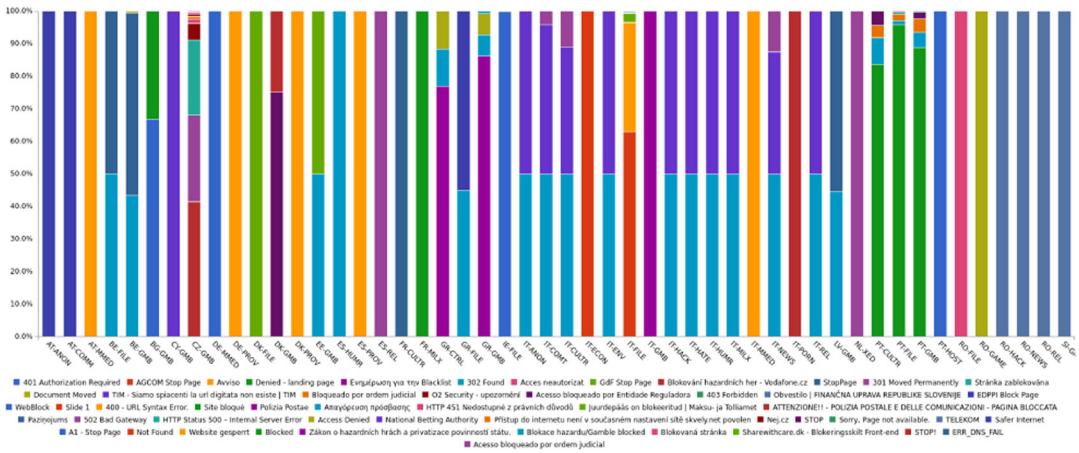

FIGURE 5 Blockpages per title and country code (Alpha-2 ISO3166) and blocked website category as depicted in Table 2. The colored bars for each country code and website category illustrate the variety of blockpages found in Open Observatory of Network Interference data.

TABLE 2 Categories of blocked websites illustrated in Figure 5 based on (Citizen Lab et al., 2014).

Category description	Code	Description
Anonymization, and circumvention tools	ANON	Used for anonymization, circumvention, proxy-services, and encryption.
Communication Tools	COMT	Sites, and tools for individual, and group communications. Includes webmail, VoIP, instant messaging, chat, and mobile messaging applications.
Control content	CTRL	Benign or innocuous content used as a control.
Culture	CULTR	Content relating to entertainment, history, literature, music, film, books, satire, and humor.
E-commerce	COMM	Websites of commercial services, and products.
Economics	ECON	General economic development, and poverty-related topics, agencies, and funding opportunities.
Environment	ENV	Pollution, international environmental treaties, deforestation, environmental justice, disasters, etc.
File-sharing	FILE	Sites, and tools used to share files, including cloud-based file storage, torrents, and P2P file-sharing tools.
Gambling	GMB	Online gambling sites. Includes casino games, sports betting, etc.
Gaming	GAME	Online games, and gaming platforms, excluding gambling sites.
Government	GOVT	Government-run websites, including military sites.
Hacking Tools	HACK	Sites dedicated to computer security, including news, and tools. Includes malicious, and nonmalicious content.
Hate Speech	HATE	Content that disparages particular groups or persons based on race, sex, sexuality or other characteristics.
Hosting, and Blogging Platforms	HOST	Web hosting services, blogging, and other online publishing platforms.
Human Rights Issues	HUMR	Sites dedicated to discussing human rights issues in various forms. Includes women's rights, and rights of minority ethnic groups.
LGBT	LGBT	A range of gay-lesbian-bisexual-transgender queer issues (excluding pornography).
Media sharing	MMED	Video, audio or photo sharing platforms.
News Media	NEWS	This category includes major news outlets (BBC, CNN, etc.) as well as regional news outlets, and independent media.
Online Dating	DATE	Online dating services which can be used to meet people, post profiles, chat, etc.
Pornography	PORN	Hard-core, and soft-core pornography.
Provocative Attire	PROV	Websites which show provocative attire, and portray women in a sexual manner, wearing minimal clothing.
Religion	REL	Sites devoted to discussion of religious issues, both supportive, and critical, as well as discussion of minority religious groups.

(Continues)

TABLE 2 (Continued)

Category description	Code	Description
Sex Education	XED	Includes contraception, abstinence, STDs, healthy sexuality, teen pregnancy, rape prevention, abortion, sexual rights, and sexual health services.
Terrorism, and Militants	MILX	Sites promoting terrorism, violent militant or separatist movements.

Blocklists

A blocklist is a collection, put together by network regulators, of web addresses which may violate laws or regulations. For the sake of correct terminology and inclusive language, we use the word blocklist, instead of the word blacklist, used by almost all authorities in the EU countries that release such lists. During our research, we were able to find and identify official blocklists issued by 15 countries and one unofficial blocklist that is not issued by a country's authority, but is based on a court order. In total, we detected 23 blocklists with entries of websites from the categories regarding copyright, gambling, health, phishing, and tobacco. We developed a system that downloads, cleans, and assembles the blocklist files into Python Pandas data frames. This eases the data analysis and helps to get reproducible new versions of the blocklists in case of an update.

The majority of the blocklists are released in a PDF file format which makes them nonideal for immediate processing. We converted these blocklists with the PyPDF2 and tabula-py Python libraries. We manually inspected the blocklist files and extracted relevant areas that include the blocked entries. Extracting data from PDF files in various languages and character encodings is a cumbersome process, but once the relevant areas of interest are isolated, we can then convert all the blocklists into data frames. The second most used file format, text file, is considerably easier to transform into data frames. Fewer blocklists are in HyperText Markup Language (HTML) and Comma-separated Values (CSV) file format; one is in Excel Workbook (XLSX) and another one in Extensible Markup Language (XML). All of these are simpler to extract into data frames.

We scanned them and thematically categorized the blocklists under the following categories: copyright, IP address based, health (including medical), gambling, phishing, or tobacco-related websites. The results are presented in Table 3 and in Figure 6 and follow the notation:

$$\{CountryName\,(BlocklistType)\}$$

The data for the phishing blocklist of Poland has been omitted from Figure 7 because the additional 14,522 entries would make the Figure look odd. All EU countries publish a gambling blocklist, most publish a copyright blocklist, Italy publishes a blocklist for tobacco-related websites, Denmark publishes a blocklist for medical-related websites, and Poland a blocklist with website entries related to phishing attacks (not included in Figure 6). Finally, the Netherlands releases an IP-based blocklist as an additional blocklist to their domain-name-based blocklist. The other 22 blocklists all contain only domain names (several include subdomains).

Because many countries publish more than one blocklist, we created Figure 7 to illustrate the cumulative number of blocklist entries per country. The data show that Poland has almost 15,000 entries (14,494) without including the phishing blocklist (with 14,522 entries), followed by Cyprus with 14,000 entries (13,789) and Italy with more than 11,000

TABLE 3 Detected blocklists per country.

Country	Entity	Type	Format	Reference
Austria	Telekom Control Commission	Copyright[a]	PDF	Telekom Control Kommission (TKK) (2023)
Belgium	Gaming Commission	Gambling	HTML	Belgian Gaming Commission (2021)
Bulgaria	National Revenue Agency	Gambling	PDF	NRA Gambling Authority blocklist (2021)
Croatia	Ministry of Finance and Tax Administration	Gambling	PDF	The Republic of Croatia, Ministry of Finance, Tax Administration—Blocklist (2021)
Cyprus	National Betting Authority	Gambling	TXT	Cyprus National Betting Authority, Blocklist (2021)
Czech Republic	Ministry of Finance	Gambling	PDF	Zveřejňované údaje ze Seznamu nepovolených internetových her k 29.6.2021 (2021)
Denmark	Telecom Industry Association	Copyright	CSV	Teleindustrien (2021)
Denmark	Telecom Industry Association	Gambling	CSV	Teleindustrien (2021)
Denmark	Telecom Industry Association	Health	CSV	Teleindustrien (2021)
Estonia	Republic of Tax and Customs Board	Gambling	PDF	Blocked illegal remote gambling sites: Estonian Tax and Customs Board (2021)
France	–	–	–	–
Germany	Clearinghouse Copyright on the Internet	Copyright[a]	PDF	Empfehlungen Clearingstelle Urheberrecht im Internet (2023)
Greece	Hellenic Copyright Association	Copyright	PDF	Hellenic Copyright Organization (2021)
Greece	Hellenic Gaming Commission	Gambling	XLSX	Official Webpage Of Hellenic Gaming Commission (Hgc) (2021)
Hungary	Supervisory Authority for Regulated Activities	Gambling	HTML	Blokkolt honlapok—Szerencsejáték Felü gyelet (2021)
Italy	Autonomous Administration of the State Monopoly	Gambling	TXT	Agenzia delle dogane e dei Monopoli (2021a)
Italy	Autonomous Administration of the State Monopoly	Tobacco	TXT	Agenzia delle dogane e dei Monopoli (2021b)
Italy	Authority for Communications	Copyright (!)	PDF	AGCOM (2023)

(Continues)

TABLE 3 (Continued)

Country	Entity	Type	Format	Reference
Latvia	Lotteries and Gambling Supervisory Inspection	Gambling	TXT	Lotteries and Gambling Supervisory Inspection of Latvia (2021a)
Latvia	National Electronic Mass Media Council	Copyright	TXT	National Electronic Mass Media Council of Latvia (2021)
Lithuania	Gaming Control Authority	Gambling	TXT	Gambling blocklist (2021)
Luxembourg	–	–	–	–
Malta	–	–	–	–
The Netherlands	KPN ISP	Copyright[b,c]	HTML	OONI Explorer—Open Data on Internet Censorship Worldwide: KPN Blockpage (2020)
Poland	CERT Polska	Phishing	Various	CERT Polska (2021)
Poland	Ministry of Finance	Gambling	XML	Polish Ministry of Finance (2021)
Portugal	–	–	–	–
Romania	National Gambling Authority	Gambling	TXT	Oficiul National pentru Jocuri de Noroc (2021)
Slovakia	Gambling Regulatory Authority	Gambling	CSV, PDF	Gambling Regulatory Authority of Slovak Republic (2021)
Slovenia	–	–	–	–
Spain	–	–	–	–
Sweden	–	–	–	–

[a]Assorted.
[b]IP addresses.
[c]Unofficial.

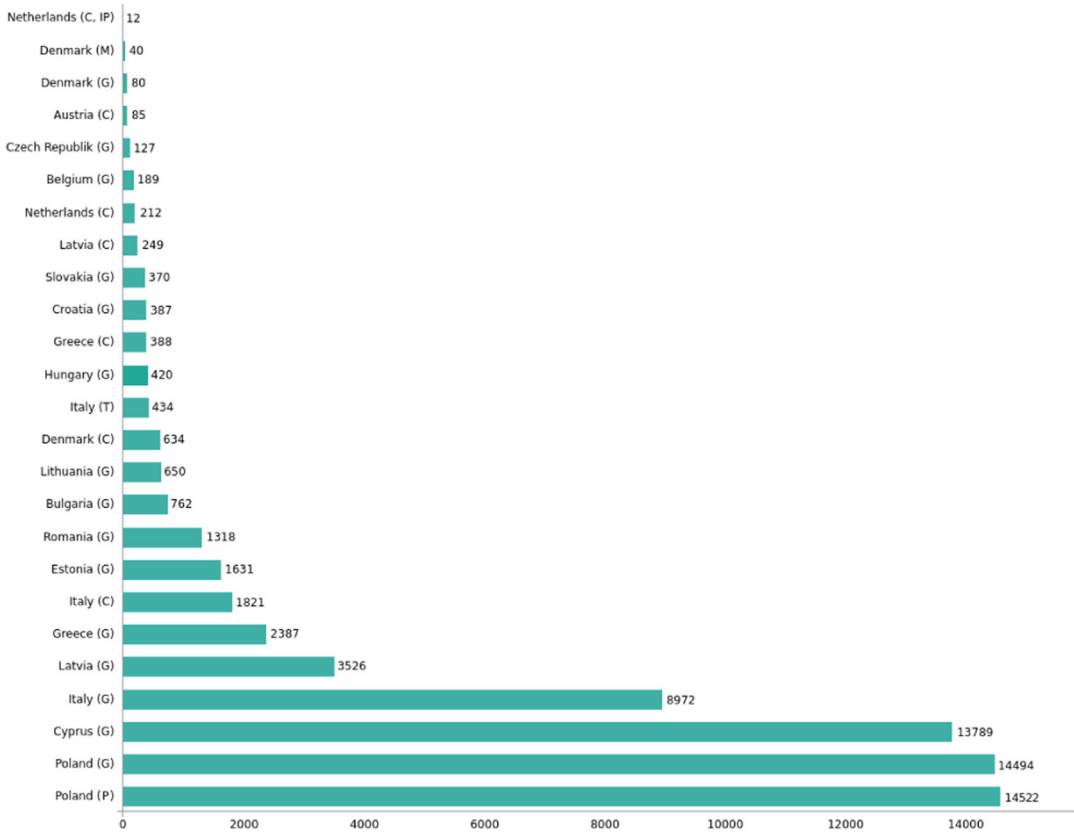

FIGURE 6 Number of entries per blocklist and blocklist type: (*C*) copyright, (*G*) gambling, (*M*) health/medical, (*IP*) IP address based, (*P*) phishing, (*T*) tobacco.

entries (11,277). This is followed by Latvia with almost 4000 entries (3775) and Greece with almost 3000 entries (2775). Both Estonia (1631) and Romania (1318) have between 2000 and 1000 blocklist entries. The remaining countries have significantly fewer than a thousand entries: Bulgaria (762), Denmark (754), Lithuania (650), Hungary (420), Croatia (387), Slovakia (370). The last four countries have blocklists with less than 220 entries, namely the Netherlands (212), Belgium (189), Czech Republic (127), and Austria (85).

We sent an e-mail query to all gambling authorities, as well as other agencies, for information on restricted websites for the countries for which we were unable to find any official or unofficial publicly available blocklist online. Apart from the ones published by the gambling regulators, countries typically have various blocklists. Due to ethical, legal, and humane considerations, we did not seek blocklists of websites that included or are related to Child Sexual Abuse Material (CSAM).

Blocklist authorities

In this section, we provide an alphabetical list of the national authorities that create blocklists and compel ISPs to block websites or services. Table 3 summarizes our results on the blocklist authorities, listing for each country the responsible entity that issues and publishes a blocklist of websites along with its type, the file format, and the relevant reference.

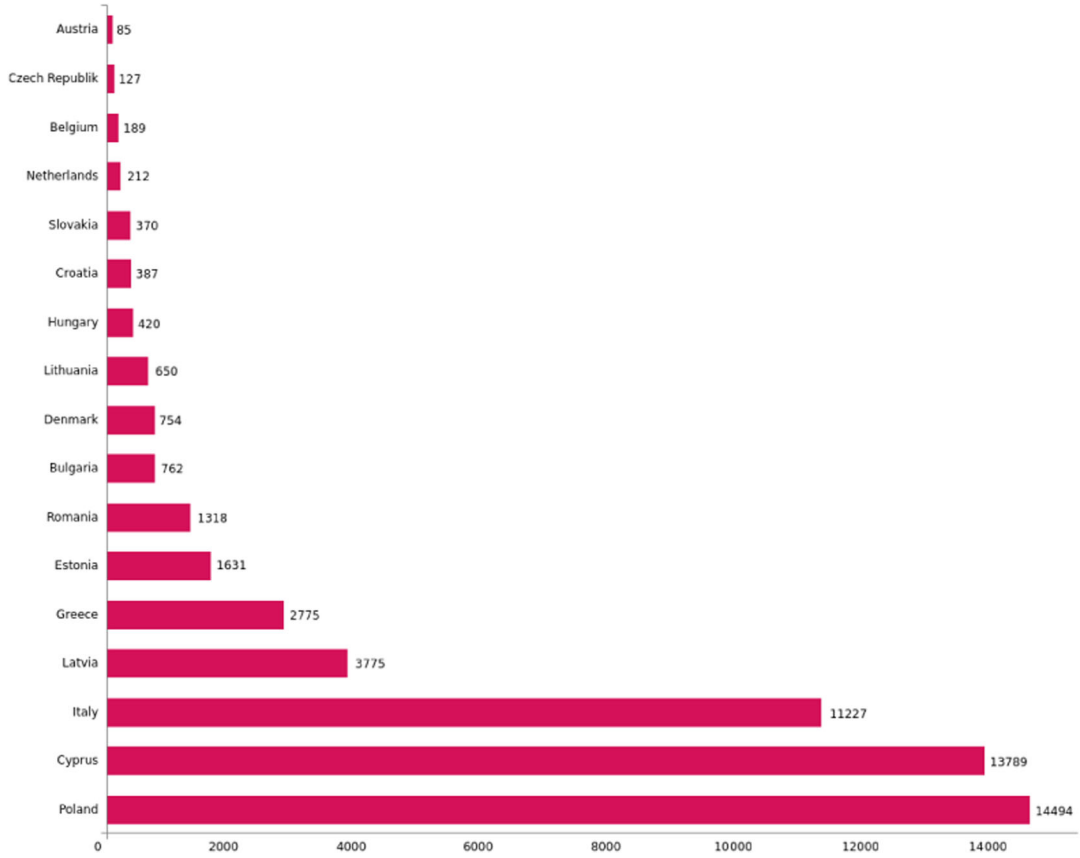

FIGURE 7 Total number of blocklist entries (cumulative) per country.

Austria

Since 2016, the regulatory institution Telekom-Control-Kommission (Telekom Control Kommission [TKK], 2023) has published on their website the national proceedings and decisions regarding net neutrality and the blocking of websites. The first relevant decision was published in 2018. It obliges ISPs to block access to websites due to alleged claims for injunctive relief under the copyright law (Telekom Control Commission, 2023). There is no official blocklist and the blocked websites can be extracted from the PDF files of the decisions. Several ISPs provide a blocklist in their websites (kabelplus GmbH, 2023a, 2023b; LIWEST Netzsperren, 2020; Magenta Redaktion, 2022), although it is unclear if the blocklists are thorough and up to date. The NRA report specifies cases of blocking based on copyright claims, typically implemented via DNS blocking (section 3.4, part II) (Austrian Regulatory Authority for Broadcasting and Telecommunications, 2021).

Belgium

We detected two different blockpages in Belgium, one for gambling websites (The Gaming Commission—The regulator of the gambling sector in Belgium, 2023) directed by the Belgian Gaming Commission and another from the Belgian Entertainment Association for

media content deemed illegal according to Belgian legislation. The error message for the blockpage links to a website in the source code of the blockpage that is dysfunctional (https://onlinefairplay.info/) and we were unable to obtain any information from the authority's website (http://belgianentertainment.be/) as it is also inoperative. The Belgian Institute for Postal Services and Telecommunications mentioned in their yearly report that there is no blocking of services or applications (section 5.117) (Belgian Institute for Postal Services and Telecommunications, 2021). The first blocklist entries date back to February 2012, as stated in the official website of the Belgian Gaming Commission (Belgian Gaming Commission, 2021).

Bulgaria

The National Revenue Agency in Bulgaria is responsible for publishing and issuing the gambling blocklist (NRA Gambling Authority blocklist, 2021). According to the blocklist file the first released blocked entry took place in June 2013 (NRA Gambling Authority blocklist, 2021). In its annual report the communications regulation commission mentions that access to websites and content is blocked only in accordance with the national legislative acts (section 1.2) (Communications Regulation Commission [CRC], 2021).

Croatia

The Ministry of Finance Tax Administration is the responsible entity for the release and publication of the gambling blocklist. It is issued as a PDF file and contains the domain names with their subdomains along with the issue date of the blocking order for each entry in the blocklist. According to the blocklist, the first blocked entry appeared at the end of May 2019 (The Republic of Croatia, Ministry of Finance, Tax Administration—Blocklist, 2021). There is no mention of Internet blocking in the country in the annual report issued by the Croatian Regulatory Authority for Network Industries (HAKOM, 2021).

Cyprus

The National Betting Authority of the Republic of Cyprus is responsible for publishing and releasing the gambling blocklist in text file format (Cyprus National Betting Authority, Blocklist, 2021). It was established as an independent authority in 2012 and although the law was issued in 2012, the first public release of the blocklist was issued in February 2013 (Ververis et al., 2017). In the annual report published by the Office of the Commissioner of Electronic Communications and Postal Regulation in Cyprus there is no mention of any Internet blocking taking place (Cyprus Office of the Commissioner of Electronic Communications and Postal Regulation, 2021).

Czech Republic

The Ministry of Finance of the Czech Republic is responsible for issuing and publishing the blocklist of gambling websites in the country. The first blocked entry appeared in July 2017; 15 versions of the blocklist are already published, given the file name prefix (*v15*) (Zveejovan daje ze Seznamu nepovolench internetovch her k 29.6.202Z, 2021). There is no

report of any blocking in the report of the Czech telecommunications authority (Czech Telecommunication Office, 2021).

Denmark

The Telecom Industry Association of Denmark releases a number of blocklists based on Danish court orders. Three different blocklist categories exist: i. the game category contains gambling websites; ii. the health category with medical and health-related websites; and iii. the intellectual property rights category with websites related to copyright infringement. All blocklists are published in the CSV file format, and a PDF file provides the date of each entry added to the blocklist. The Danish Energy Agency sent out a questionnaire to 40 ISPs in Denmark on the grounds of the EU net neutrality regulation. 30% of the ISPs stated that they are partly blocking access to the Internet. Specifically, the ISPs mentioned blocking access to CSAM websites with extremist content, or calls for terror. Further, the ISPs mentioned blocking traffic to malicious servers related to COVID-19 crime (section 4.1) (Danish Energy Agency, 2021).

Estonia

The Republic of Estonia's Tax and Customs Board is responsible for issuing and publishing the blocklist of gambling websites in the country. It is distributed as a PDF file and is publicly available to download (Blocked illegal remote gambling sites: Estonian Tax and Customs Board, 2021). The annual report of the Estonian consumer protection and technical regulatory authority fails to mention any Internet blocking in the country (Estonian Consumer Protection and Technical Regulatory Authority, 2021).

France

In France, the National Commission on Informatics and Liberty publishes yearly reports on the administrative blocking of websites. The reports give an overview of the blocked websites related to terrorism and CSAM (Contrôle du blocage administratif des sites: la personnalité qualifiée présente son 5ème rapport d'activité, 2021). They have appointed a person to verify the validity of requests for removal of content and blocking made by the central office for combating information and communication technology crime. However they do not provide details as to which websites have been blocked, but only statistical information on the number of requests to block websites. The latest report covers the period from February to December 2019, and mentions that 18,177 blocking orders were made. Of these, 420 requests were related to blocked websites, 11,874 for content removal, and 5,883 for dereferencing of e-mail addresses (France: Freedom on the Net 2020 Country Report: Freedom House, 2021). Moreover, there is no mention of Internet blocking in France's Electronic Communications, Postal and Print Media Distribution's NRA annual report (Arcep, 2021).

Germany

Clearinghouse Copyright on the Internet is an independent body established by ISPs and rights holders. Its purpose is to review and propose the blocking of websites according to

certain criteria and requirements related to copyright infringement. As mentioned on its website, a review board, at the request of the copyright holder, reviews the copyright allegedly infringing website and, if the requirements are met, recommends DNS blocking. They publish the recommendations for blocking domains on their website and the first entry appeared in February 2021 (Empfehlungen Clearingstelle Urheberrecht im Internet, 2023). According to the Federal Network Agency's annual report on net neutrality, there is no national law in Germany requiring ISPs to implement blocking in their networks. An unnamed (in the report) ISP was required to block access to some (unspecified) websites by means of DNS blocking due to a court ruling (section 3.1.2) (Bundesnetzagentur, 2020).

Greece

The annual report of the NRA in Greece (EETT, 2020) mentions that ISPs in the country block websites based on two public blocklists according to the laws related to the protection of intellectual property and blocking of gambling websites (Hellenic Copyright Organization, 2021; Official Webpage Of Hellenic Gaming Commission [Hgc], 2021). Additionally, the report mentions that ISPs block domain names to protect against phishing attacks and block IP addresses to protect their internal network and defend against distributed denial of service attacks. A user who visits one of the websites listed in the blocklist gets redirected (with an HTTP 301 redirect) to the websites of the blocking authorities. The servers of the authorities may potentially collect IP addresses and further information of users trying to access the blocked websites. Previous research observed that ISPs implemented their own blocking pages without redirecting the users to the website of the gambling regulation authority when they try to access a website on the blocklist (Ververis et al., 2015).

Hungary

The Supervisory Authority for Regulated Activities in Hungary is responsible for issuing and releasing a public blocklist for gambling websites (Blokkolt honlapok—Szerencsejáték Felü gyelet, 2021). There is no mention of the blocklist in the annual report published by the national media and communications authority (National Media and Communications Authority, 2021).

Italy

In Italy, we discovered three publicly available blocklists issued by two different entities. The Autonomous Administration of the State Monopoly lists websites related to gambling (Agenzia delle dogane e dei Monopoli, 2021a) and tobacco products (Agenzia delle dogane e dei Monopoli, 2021b). The Authority for Communications responsible for the blocklist of copyright infringement cases (AGCOM, 2023). There is no mention of any blocking in the NRA annual report (AGCOM, 2021).

Latvia

The Lotteries and Gambling Supervisory Inspection is the responsible authority for issuing and publicly releasing a gambling blocklist in Latvia. The first blocked entries appeared in August 2014 (Lotteries and Gambling Supervisory Inspection of Latvia, 2021b).

We discovered another blocklist published by the National Electronic Mass Media Council of Latvia with entries related to copyright infringement. Both blocklists are released in a text file format (National Electronic Mass Media Council of Latvia, 2021). The annual report published by the Public Utilities Commission didn't report any blocking (The Public Utilities Commission, 2021).

Lithuania

The Gaming Control Authority under the Ministry of Finance is the responsible authority for issuing the gambling blocklist of websites in Lithuania. The first entries were published in January 2016 (Gambling blocklist, 2021) in a text file format. However, there is no reference to blocking in the annual report (Communications Regulatory Authority of the Republic of Lithuania, 2021) published by the Communications Regulatory Authority of the Republic of Lithuania.

Malta

An e-mail communication from the Malta Gaming Authority (Malta Gaming Authority, 2021) revealed that they do not have the authority to block websites. However, they cooperate with Malta's police force to stop criminal gambling activity. Investigations and prosecutions are then carried out by the police, assisted by the Authority as necessary. Therefore, any repercussions (including website blocking) of illegal activities or services fall under the jurisdiction of the Malta police. The annual report of the Malta Communication Authority mentions an ongoing investigation to block specific IP addresses (undefined in the report), without saying that there was any website blocking (Malta Communications Authority, 2021).

The Netherlands

A blockpage (OONI Explorer—Open Data on Internet Censorship Worldwide: KPN Blockpage, 2020) in OONI network measurements probed on the KPN ISP mentions that the judge for provisional legal protection in Midden-Nederland ruled in January 2018 that The Pirate Bay's website should be blocked on all KPN networks including Telfort, Simyo, and KPN Hotspots. The decision lists several IP addresses, domains and subdomains that ISPs must block. The same blockpage mentions that the judicial decision (Central Netherlands Court, 2021) was also sent to other ISPs. The unofficial blocklist extracted from the blockpage (OONI Explorer—Open Data on Internet Censorship Worldwide: KPN Blockpage, 2020) lists 12 IP addresses (IPv4 and IPv6) and a list of 212 domains and subdomains that are proxies or mirrors of The Pirate Bay website. The Authority for Consumers and Markets released the annual NRA report without providing any information about the blocking of websites or services (Authority for Consumers & Markets, 2021).

Poland

The NRA report of the Office of Electronic Communications (Urząd Komunikacji Elektronicznej, 2020) mentions that ISPs are obliged to block gambling websites. The Polish Ministry of Finance releases the gambling blocklist (Polish Ministry of Finance, 2021), provided as a REST XML service that can be retrieved programmatically and includes the

documentation of its specification. Another blocklist (called Warning List) (CERT Polska, 2021) has been created to block websites related to phishing activities. An agreement was made in March 2020 with the Minister of Digital Affairs, the Office of Electronic Communications and National Research Institute, and the four largest mobile network operators, Orange, T-Mobile, P4, and Polkomtel, to block specific websites (UKE przystąpił do porozumienia chroniącego abonentów—Urząd Komunikacji Elektronicznej, 2021). The CERT Polska team is responsible for the maintenance and release of this blocklist. On their website, they have created a form where individuals can report suspicious websites, and each report is manually verified by at least two persons. The blocklist is released in various file formats, updated every 5 min, and the full specification of the API is available on their website (CERT Polska, 2021).

Romania

The Romanian National Gambling Authority has released a gambling blocklist since 2015 (Oficiul National pentru Jocuri de Noroc, 2021). It is available on their website in a text file format. They also provide a helper script (written in the PHP programming language) that replaces the A and NS DNS records of the domain (and the *www* subdomain) for all the entries found on the blocklist, compatible with the BIND DNS server configuration. According to the annual report (ANCOM, 2021) of the National Authority for Administration and Regulation in Communications, that entity issued 15 blocking orders related to COVID-19 fake news, as well as protection and prevention measures during the state of emergency that ended in May 2020 (The National Authority for Administration and Regulation in Communications [ANCOM], n.d). The gambling blocklist is not mentioned in the report.

Slovakia

The annual report (Slovak Republic Regulatory Authority for Electronic Communications and Postal Services, 2021) published by the Regulatory Authority for Electronic Communications and Postal Services mentions that ISPs block access to applications or services in the event of illegal content as ruled by European or national legislation. Online gambling websites without a Slovak license are blocked, as well as websites that host CSAM. The Slovakian Gambling Regulatory Authority is responsible for issuing and publishing the gambling blocklist, and its first entry appeared in August 2019 (Gambling Regulatory Authority of Slovak Republic, 2021).

CONCLUSION AND FURTHER DISCUSSION

This study sheds light on how website blocking occurs in the European Union. The process of gathering data involved several steps and sources, sometimes not easily available. Some of the data sources were provided after e-mail communication with the regulators. The research identified blockpages and blocklists in jurisdictions across Europe. In our blocklist evaluation study (in the Blocklists section) we detected different types of blocklist publication and distribution methods.

We identified some issues with the reporting of such blocklists. Most regulators and authorities are using PDF files, others publish the blocklists on their websites, and a few release them in a CSV or other file format. All of these approaches are cumbersome and

lead to error-prone processes for the ISPs maintaining updated lists of websites and services to block. This may result in over- and under-blocking (Ververis et al., 2015). Besides, most NRAs do not describe in their reports what blocking they do. Only a few authorities publish even limited details on the resources and websites blocked, with no references to the blocklists. Details for each country are provided in the Data analysis results section. A well-designed system can help address a number of these problems related to Internet regulations and blocking of websites and services, albeit the issue is not just technological, but may involve political and legal questions.

We focused on the overlooked trend of EU member states deploying surveillance and network infrastructures to adhere to the EU legislation. We focused on the publication and release of EU blocklists and website blocking in 2020. Based on historical network measurements data by OONI, this paper provides evidence that countries in the EU not only use blocklists as a means of blocking access to websites but also block different types and categories of websites and services that are not included in the publicly available (identified) blocklists.

All countries publish a gambling blocklist, most publish a copyright blocklist, Italy publishes a blocklist for tobacco-related websites, Denmark publishes a blocklist for medical websites, and Poland publishes a blocklist with entries on phishing websites. Finally, the Netherlands publishes IP-based blocklist as an additional blocklist to their domain-name-based blocklist. The other 22 blocklists all list only domain names or URLs.

In terms of the cumulative number of blocklist entries per country, Poland has just over 29,000 entries (including the phishing blocklist), followed by Cyprus with almost 14,000 entries and Italy with more than 11,000 entries. Latvia, Greece, Estonia, and Romania, with between 4000 entries and 1000 entries in blocklists, make up the midfield. The remaining countries have significantly fewer than a thousand entries.

We also analyzed data from the OONI project, a platform for detecting Internet censorship that has been actively developed since 2012. OONI network measurements are carried out on an ad-hoc basis by volunteers. The data submitted still rely on the availability and willingness of people to conduct network measurements, notwithstanding the software's ongoing improvement. Although OONI has collected and released data on network measurements from all countries worldwide, getting longitudinal network measurements is challenging. It is important that quantitative network measurements be carried out from diverse locations even for the same ISPs and ASes.

Regulatory sanctions and restriction to access to online resources

As the literature demonstrates, governments and state actors have used Internet censorship to influence political discourse and favor businesses under their own control (Greengard, 2010). Citizens can also potentially be denied access to services as a result of local regulatory laws, financial reasons, or because their country has fallen under sanctions and prohibits foreign companies from operating within their jurisdiction (Ververis et al., 2019). Some authors suggest that, having been characteristic of repressive regimes, Internet censorship could become almost ubiquitous in both democratic and authoritarian states (Bambauer, 2013).

As example, the EU has imposed a number of sanctions in response to Russia's invasion of Ukraine. In particular, the EU Council adopted Decision 2022/351, imposing new restrictive measures against the Russian state media and their subsidiaries (EU sanctions against Russia following the invasion of Ukraine, 2022). The Council decision does not specify exact websites, domains, or URLs to be blocked, but rather says 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). Annex XV lists only the names of the entities or bodies, specifically: *RT- Russia Today English*, *RT- Russia Today UK*, *RT- Russia Today Germany RT- Russia Today France*, *RT- Russia Today Spanish* and *Sputnik*.

This prohibition forces ISPs to make their own decisions about which websites and services to block, which is a difficult process with many implementation gaps and the risk of under- or over-blocking (Formal Internet Censorship: Copyright blocking injunctions, 2019). The EU council also calls for blocking content distributed via cable, satellite, ISPs, and IP-TV connections on video-sharing websites in addition to the websites owned by these entities. In reality, such extensive service blocking is impractical and results in the excessive over-blocking of websites and services (Formal Internet Censorship: Copyright blocking injunctions, 2019; Open Rights Groups, 2012; Ververis et al., 2015).

ISPs in the EU are already employing various blocking techniques to block the websites of *rt.com* and *sputniknews.com*. The majority of them make use of their current blocking infrastructure, including the same blocking pages that falsely claim the websites are blocked because of copyright infringement, gambling, or other laws (The latest crazy law, 2022). These are similar to the blocking pages examined in The Detected blockpages section which have nothing to do with the blocking of these websites. The blocking infrastructure requires a significant number of labor hours and hardware infrastructure to be implemented and maintained (The latest crazy law, 2022). For instance, this is the situation with smaller ISPs in the United Kingdom, where new Internet service sanctions in the country require ISPs to block access to the websites and services listed in the sanctions. Failure to do so can result in fines of up to £1,000,000 (Ofcom, 2022; The latest crazy law, 2022).

Limitations

The conclusions of this paper have limitations which may prompt future research, especially regarding other forms of Internet censorship and further methods of network interference that may require a legal and policy analysis from the principles of network neutrality and Open Internet.

ACKNOWLEDGMENTS

The authors would like to thank Richard Schmeidler for the proofreading and the anonymous reviewers for their valuable contributions to the paper. Open Access funding enabled and organized by Projekt DEAL.

ORCID

Vasilis Ververis http://orcid.org/0000-0002-7681-1147

ENDNOTE

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

REFERENCES

Aceto, G., Botta, A., Pescapè, A., Awan, M. F., Ahmad, T., & Qaisar, S. (2016). Analyzing Internet censorship in Pakistan. In *Research and technologies for society and industry* (pp. 1–6). IEEE. https://wpage.unina.it/giuseppe.aceto/pub/aceto2016analyzing.pdf

AGCOM. (2021, June). *Report on the activities carried out by the authority in the field of open Internet*. https://ec.europa.eu/newsroom/dae/redirection/document/78867
AGCOM. (2023, January). *Provvedimenti*. https://www.agcom.it/provvedimenti-a-tutela-del-diritto-d-autore
Agenzia delle dogane e dei Monopoli. (2021a, June). https://www1.adm.gov.it/files_siti_inibiti/elenco_siti_inibiti.txt
Agenzia delle dogane e dei Monopoli. (2021b, June). https://www1.agenziadoganemonopoli.gov.it/files_siti_inibiti_tabacchi/elenco_siti_inibiti.txt
Al-Saqaf, W. (2016). Internet censorship circumvention tools: Escaping the control of the Syrian regime. *Media and Communication*, *4*(1), 39–50.
ANACOM. (2021, June). *Report on net neutrality—May 2020 to April 2021*. https://ec.europa.eu/newsroom/dae/redirection/document/78917
ANCOM. (2021, June). *Monitoring compliance with Regulation (EU) No 2015/2120 on open Internet access 01 May 2020—30 April 2021*. https://ec.europa.eu/newsroom/dae/redirection/document/78877
Anderson, C. (2012). *The hidden Internet of Iran: Private address allocations on a national network* (Tech. rep.). https://arxiv.org/pdf/1209.6398v1.pdf
Anderson, C. (2013). *Dimming the Internet: Detecting throttling as a mechanism of censorship in Iran* (Tech. rep.). University of Pennsylvania. https://arxiv.org/pdf/1306.4361v1.pdf
Angelopoulos, C. (2009). Filtering the Internet for copyrighted content in Europe. In *IRIS plus 2009-4*. European Audiovisual Observatory.
Arcep. (2021, July). *The state of the Internet in France*. https://ec.europa.eu/newsroom/dae/redirection/document/78869
Aryan, S., Aryan, H., & Halderman, J. A. (2013). Internet censorship in Iran: A first look. In *Free and Open Communications on the Internet*. Usenix. https://censorbib.nymity.ch/pdf/Aryan2013a.pdf
Austrian Regulatory Authority for Broadcasting and Telecommunications. (2021, July). *RTR net neutrality report 2021*. https://ec.europa.eu/newsroom/dae/redirection/document/78845
Authority for Consumers & Markets. (2021, June). *2020–2021 annual report on net neutrality*. https://ec.europa.eu/newsroom/dae/redirection/document/78871
Bambauer, D. E. (2013). Censorship v3.1. In *IEEE Internet Computing* (pp. 26–33). https://ieeexplore.ieee.org/document/6415890
Belgian Gaming Commission. (2021, June). *Blocklist*. https://www.gamingcommission.be/opencms/opencms/jhksweb_en/establishments/Online/blacklist/index.html
Belgian Institute for Postal Services and Telecommunications. (2021, June). *Report regarding the monitoring of net neutrality in Belgium (period from 1 May 2020–30 April 2021)*. https://ec.europa.eu/newsroom/dae/redirection/document/78849
Blocked illegal remote gambling sites: Estonian Tax and Customs Board. (2021, January). https://www.emta.ee/eng/private-client/land-vehicle-forest-gambling/remote-gambling-sites
Blokkolt honlapok—Szerencsejáték Felü gyelet. (2021, June). https://szf.gov.hu/hatosag/blokkolt-honlapok
Bundesnetzagentur. (2020, April). *Net neutrality in Germany annual report 2019/2020*. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68751
Bundesnetzagentur. (2021, July). *Net neutrality in Germany annual report 2020/2021*. https://ec.europa.eu/newsroom/dae/redirection/document/78865
Busch, A., Theiner, P., & Breindl, Y. (2018). Internet censorship in liberal democracies: Learning from autocracies? In J. Schwanholz, T. Graham, & P.-T. Stoll (Eds.), *Managing democracy in the digital age* (pp. 11–28). Springer International Publishing. https://doi.org/10.1007/978-3-319-61708-4_2
Central Netherlands Court. (2021, June). *ECLI:NL:RBMNE:2018:114, Rechtbank Midden-Nederland, C/16/448423/KG ZA 17-382*. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2018:114
CERT Polska. (2021, June). *Lista ostrzeżeń przed niebezpiecznymi stronami*. https://www.cert.pl/posts/2020/03/ostrzezenia_phishing/#files
Chaabane, A., Chen, T., Cunche, M., Cristofaro, E. D., Friedman, A., & Kaafar, M. A. (2014). Censorship in the wild: Analyzing Internet filtering in Syria. In *Internet Measurement Conference*. ACM. https://conferences2.sigcomm.org/imc/2014/papers/p285.pdf
Chen, L., Zhang, C., & Wilson, C. (2013). Tweeting under pressure: Analyzing trending topics and evolving word choice on Sina Weibo. In *Conference on Online Social Networks*. ACM. https://cbw.sh/static/pdf/weibo-cosn13.pdf
Citizen Lab and Others. (2014). *URL testing lists intended for discovering website censorship*. https://github.com/citizenlab/test-lists#citation
Clayton, R., Murdoch, S. J., & Watson, R. N. M. (2006). Ignoring the great firewall of China. In *Privacy enhancing technologies* (pp. 20–35). Springer. https://www.cl.cam.ac.uk/~rnc1/ignoring.pdf
Commission for Communications Regulation. (2021, June). *Implementation of EU Open Internet Access Regulations in Ireland*. https://ec.europa.eu/newsroom/dae/redirection/document/78859

Communications Regulation Commission (CRC). (2021, June). *Annual report on the implementation of the regulation (EC) 2015/2120 for 2020*. https://ec.europa.eu/newsroom/dae/redirection/document/78849
Communications Regulatory Authority of the Republic of Lithuania. (2021, June). *Open internet and implementation of the regulation (EU) 2015/2120 in Lithuania*. Report to the European Commission. https://ec.europa.eu/newsroom/dae/redirection/document/78860
Contrôle du blocage administratif des sites: la personnalité qualifiée présente son 5ème rapport d'activité. (2021, June). https://www.cnil.fr/fr/controle-du-blocage-administratif-des-sites-la-personnalite-qualifiee-presente-son-5eme-rapport
Council of the European Union. (2015, November). *Regulation (EU) 2015/2120 of the European Parliament and of the Council*. https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/9277-berec-guidelines-on-the-implementation-o_0.pdf
Cyprus National Betting Authority, Blocklist. (2021, June). https://nba.gov.cy/wp-content/uploads/BlockingListLatest.txt
Cyprus Office of the Commissioner of Electronic Communications and Postal Regulation. (2021, August). Annual report 2021 on Open Internet. https://ec.europa.eu/newsroom/dae/redirection/document/78851
Czech Telecommunication Office. (2021, August). *Report of the Czech telecommunications authority (for the period from 1st of May 2020 to 30th of April 2021)*. https://ec.europa.eu/newsroom/dae/redirection/document/78853
Danish Energy Agency. (2021, June). *The Danish Energy Agency's supervision of the EU regulation on access to the open Internet*. https://ec.europa.eu/newsroom/dae/redirection/document/78855
Dunna, A., O'Brien, C., & Gill, P. (2018). Analyzing China's blocking of unpublished Tor bridges. In *Free and Open Communications on the Internet*. Usenix. https://www.usenix.org/system/files/conference/foci18/foci18-paper-dunna.pdf
EETT. (2020, June). *Έκθεση Ανοικτού Διαδικτύου 2019-2020*. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68329
Empfehlungen Clearingstelle Urheberrecht im Internet. (2023, January). https://cuii.info/empfehlungen
Ensafi, R., Winter, P., Mueen, A., & Crandall, J. R. (2015). Analyzing the great firewall of China over space and time. *Privacy Enhancing Technologies*, *2015*(1), 61–76.
Estonian Consumer Protection and Technical Regulatory Authority. (2021, June). *Report on the Estonian Consumer Protection and Technical Regulatory Authority's work on the implementation of the EU Net Neutrality Regulation*. https://ec.europa.eu/newsroom/dae/redirection/document/78857
EU sanctions against Russia following the invasion of Ukraine. (2022, March). https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-solidarity-ukraine/eu-sanctions-against-russia-following-invasion-ukraine_en
Evdokimov, L. (2019). *metadb s3 tarx: Fetch public OONI metadb backup from AWS S3 Open Data*. https://github.com/ooni/sysadmin/blob/master/scripts/metadb_s3_tarx
Filastò, A. (2018). *OONI data license*. https://github.com/ooni/license/blob/master/data/CC4.0-BY-NC-SA.md
Filastò, A. (2019). *OONI MetaDB Sharing*. https://github.com/ooni/sysadmin/blob/master/docs/metadb-sharing.md
Formal Internet Censorship: Copyright blocking injunctions. (2019, February). https://www.openrightsgroup.org/blog/formal-internet-censorship-copyright-blocking-injunctions
France: Freedom on the Net 2020 Country Report: Freedom House. (2021, June). https://freedomhouse.org/country/france/freedom-net/2020
Gambling blocklist. (2021, June). Gaming Control Authority under the Ministry of Finance of the Republic of Lithuania. https://lpt.lrv.lt/uploads/lpt/documents/files/neleg.txt
Gambling Regulatory Authority of Slovak Republic. (2021, June). https://www.urhh.sk/sk/web/guest/zoznam-zakazanych-sidel
Gebhart, G., Author, A., & Kohno, T. (2017). Internet censorship in Thailand: User practices and potential threats. In *European Symposium on Security & Privacy*. IEEE. https://homes.cs.washington.edu/~yoshi/papers/GebhartEtAl-IEEEEuroSP.pdf
Gosain, D., Agarwal, A., Shekhawat, S., Acharya, H. B., & Chakravarty, S. (2017). Mending wall: On the implementation of censorship in India. In *SecureComm*. Springer. https://censorbib.nymity.ch/pdf/Gosain2017a.pdf
Greengard, S. (2010). Censored! *Communications of the ACM*, *53*, 16–18. https://dl.acm.org/doi/10.1145/1785414.1785423
HAKOM. (2021, June). *Annual report on the national implementation of the regulation (EU) 2015/2120 (period from 1th of May 2020–30th of April 2021*. https://ec.europa.eu/newsroom/dae/redirection/document/78852
Hellenic Copyright Organization. (2021, June). https://opi.gr/images/epitropi/edppi_list_v8.pdf
Holowczak, J., & Houmansadr, A. (2015). CacheBrowser: Bypassing Chinese censorship without proxies using cached content. In *Computer and communications security*. ACM. https://people.cs.umass.edu/~amir/papers/CacheBrowser.pdf

Hounsel, A., Mittal, P., & Feamster, N. (2018). Automatically generating a large, culture-specific blocklist for China. In *Free and Open Communications on the Internet*. Usenix. https://www.usenix.org/system/files/conference/foci18/foci18-paper-hounsel.pdf

Iszaevich, G. E. W. (2019). Distributed detection of Tor directory authorities censorship in Mexico. In *International Conference on Networks*. Iaria. https://tics.site/proceedings/2019a/icn_2019_6_20_38010.pdf

kabelplus GmbH. (2023a, January). *Gesperrte Websites wegen Urheberrechtsverletzungen*. https://www.kabelplus.at/specialpages/gesperrte-websites-wegen-urheberrechtsverletzungen-aspx

kabelplus GmbH. (2023b, January). *Update—Übersicht der gesperrten Webseiten (VO 350/2022)*. https://www.kabelplus.at/privat/service/neuigkeiten/gesperrte-websites

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *107*(2), 1–18. https://gking.harvard.edu/files/censored.pdf

King, G., Pan, J., & Roberts, M. E. (2014). Reverse-engineering censorship in China: Randomized experimentation and participant observation. *Science*, *345*, 1–10. https://gking.harvard.edu/publications/randomized-experimental-study-censorship-china

Knockel, J., Crete-Nishihata, M., Ng, J. Q., Senft, A., & Crandall, J. R. (2015). Every rose has its thorn: Censorship and surveillance on social video platforms in China. In *Free and Open Communications on the Internet*. Usenix. https://www.usenix.org/system/files/conference/foci15/foci15-paper-knockel.pdf

Knockel, J., Ruan, L., & Crete-Nishihata, M. (2017). Measuring decentralization of Chinese keyword censorship via mobile games. In *Free and Open Communications on the Internet*. Usenix. https://www.usenix.org/system/files/conference/foci17/foci17-paper-knockel.pdf

Knockel, J., Ruan, L., & Crete-Nishihata, M. (2018). An analysis of automatic image filtering on WeChat Moments. In *Free and Open Communications on the Internet*. Usenix. https://www.usenix.org/system/files/conference/foci18/foci18-paper-knockel.pdf

LIWEST Netzsperren. (2020, March). https://netzsperre.liwest.at

Lotteries and Gambling Supervisory Inspection of Latvia. (2021a, June). *Gambling blocklist*. https://www.iaui.gov.lv/images/Blokesana/domeni.txt

Lotteries and Gambling Supervisory Inspection of Latvia. (2021b, June). *Unlicensed interactive gambling websites blocked*. https://www.iaui.gov.lv/images/Blokesana/domeni.txt

Lowe, G., Winters, P., & Marcus, M. L. (2007). *The great DNS wall of China* (Tech. rep.). New York University. https://censorbib.nymity.ch/pdf/Lowe2007a.pdf

Luxembourg Institute of Regulation. (2021, June). *Access to an open internet in Luxembourg—activity report*. https://ec.europa.eu/newsroom/dae/redirection/document/78864

Magenta Redaktion. (2022, August). *Netzsperre: Was bedeutet "Diese Seite ist gesperrt"?* Magenta. https://blog.magenta.at/internet/sicherheit/netzsperre

Malta Communications Authority. (2021, June). *Report of the Malta Communications Authority on its monitoring and findings in accordance with Article 5 of Regulation (EU) 2015/2120 concerning the European Net Neutrality Rules*. https://ec.europa.eu/newsroom/dae/redirection/document/78866

Malta Gaming Authority. (2021). https://www.mga.org.mt

Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R., & Paxson, V. (2015). An analysis of China's "Great Cannon". In *Free and Open Communications on the Internet*. Usenix. https://www.usenix.org/system/files/conference/foci15/foci15-paper-marczak.pdf

Market Regulation Department Swedish Post and Telecom Authority. (2021, June). *Open internet—annual reporting 2020/2021*. https://ec.europa.eu/newsroom/dae/redirection/document/78878

Morshed, M. B., Dye, M., Ahmed, S. I., & Kumar, N. (2017). When the Internet goes down in Bangladesh. In *Computer-supported cooperative work and social computing*. ACM. https://nehakumardotorg.files.wordpress.com/2014/03/p1591-bin-morshed.pdf

Nabi, Z. (2013). The anatomy of web censorship in Pakistan. In *Free and Open Communications on the Internet*. Usenix. https://censorbib.nymity.ch/pdf/Nabi2013a.pdf

National Electronic Mass Media Council of Latvia. (2021, June). *List of restricted domain names*. https://www.neplpadome.lv/lv/sakums/mediju-lietotajiem/ierobezoto-domenu-vardu-saraksts/

National Media and Communications Authority. (2021, June). *The state of open Internet in Hungary in 2021*. https://ec.europa.eu/newsroom/dae/redirection/document/78861

National Telecommunications and Postal Commission. (2021, July). *Open Internet report 2020–2021*. https://ec.europa.eu/newsroom/dae/redirection/document/78858

Ng, K. Y., Feldman, A., & Leberknight, C. (2018). Detecting censorable content on Sina Weibo: A pilot study. In *Hellenic Conference on Artificial Intelligence*. ACM. https://censorbib.nymity.ch/pdf/Ng2018a.pdf

Niko, A., Klaus, N., Elina, P., & Marko, P. (2021, July). *Annual net neutrality report 2021*. https://ec.europa.eu/newsroom/dae/redirection/document/79071

NRA Gambling Authority blocklist. (2021, June). https://nra.bg/wps/portal/nra/gambling/Online-hazat

Ofcom. (2022, April). *Open letter to industry about new restrictions on the provision of certain internet services to, or for the benefit of, "designated persons"*. https://www.ofcom.org.uk/_data/assets/pdf_file/0023/237218/open-letter-russia-sanctions.pdf

Office of Electronic Communications. (2021, June). *Report of the President of the Office of Electronic Communications on compliance in the Polish market with Regulation 2015/2120 on open internet access*. https://ec.europa.eu/newsroom/dae/redirection/document/78874

Official Webpage of Hellenic Gaming Commission (Hgc). (2021, June). https://www.gamingcommission.gov.gr/index.php/en

Oficiul National pentru Jocuri de Noroc. (2021, June). *Gambling Blocklist*. https://onjn.gov.ro/wp-content/uploads/Onjn.gov.ro/Acasa/BlackList/Lista-neagra.txt

Open Observatory of Network Interference (OONI). (2019). *Web Connectivity test specification*. https://github.com/ooni/spec/blob/master/nettests/ts-017-web-connectivity.md

Open Observatory of Network Interference (OONI). (2020). https://ooni.org

OONI Explorer—Open Data on Internet Censorship Worldwide: KPN Blockpage. (2020, June). https://explorer.ooni.org/m/01202006164675ba341d04b443650f0e8dd3c5b9

OONI Explorer—Open Data on Internet Censorship Worldwide. (2022, May). https://explorer.ooni.org

Open Rights Groups. (2012, May). *Mobile Internet censorship: What's happening and what we can do about it*. https://www.openrightsgroup.org/app/uploads/2020/03/MobileCensorship-webwl-1.pdf

Park, J. C., & Crandall, J. R. (2010). Empirical study of a national-scale distributed intrusion detection system: Backbone-level filtering of HTML responses in China. In *Distributed computing systems* (pp. 315–326). IEEE. https://www.cs.unm.edu/~crandall/icdcs2010.pdf

Poblet, M. (2018). Distributed, privacy-enhancing technologies in the 2017 Catalan referendum on independence: New tactics and models of participatory democracy. *First Monday*, *23*(12). https://firstmonday.org/ojs/index.php/fm/article/view/9402

Polish Ministry of Finance. (2021, June). *Rejestr domen—Rejestr Domen Służących do Oferowania Gier Hazardowych Niezgodnie z Ustawą*. https://hazard.mf.gov.pl/api/Register

Ramesh, R., Raman, R. S., Bernhard, M., Ongkowijaya, V., Evdokimov, L., Edmundson, A., Sprecher, S., Ikram, M., & Ensafi, R. (2020). Decentralized control: A case study of Russia. In *Network and distributed system security*. The Internet Society. https://www.ndss-symposium.org/wp-content/uploads/2020/02/23098.pdf

Robinson, D., Yu, H., & An, A. (2013). *Collateral freedom: A snapshot of Chinese Internet users circumventing censorship* (Tech. rep.). OpenITP. https://www.upturn.org/static/files/CollateralFreedom.pdf

Savola, P. (2015). *Internet connectivity providers as involuntary copyright enforcers: Blocking websites in particular* (p. 300). https://www.semanticscholar.org/paper/Internet-Connectivity-Providers-as-Involuntary-%3A-in-Savola/3697801a239fa9dfad86de6ee65311b202b49e4d

Schmidt-Kessen, M. J., Hörnle, J., & Littler, A. (2019). Preventing risks from illegal online gambling using effective legal design on landing pages. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3474296; Retrieved April 5, 2020, from https://www.ssrn.com/abstract=3474296

Shirazi, F., & Greenaway, K. (2009). Examining validity claims for internet filtering in Islamic Middle Eastern countries: A critical discourse analysis. In *AMCIS 2009 Proceedings*. http://aisel.aisnet.org/amcis2009/794

Slovak Republic Regulatory Authority for Electronic Communications and Postal Services. (2021, July). *Annual report on monitoring the regulation (EU) 2015/2120 of the European Parliament and of the Council*. https://ec.europa.eu/newsroom/dae/redirection/document/78879

Slovenian Regulatory Authority for Electronic Communications and Postal Services. (2021, June). *Annual report on monitoring the regulation (EU) 2015/2120 of the European Parliament and of the Council*. https://ec.europa.eu/newsroom/dae/redirection/document/78880

State Secretariat for Telecommunications, Digital Infrastructures of the Ministry of Economic Affairs, and Digital Transformation. (2021, July). *Report on Spain's supervision of European regulations on the open internet access (net neutrality)*. https://ec.europa.eu/newsroom/dae/redirection/document/78882

Tanash, R. S., Chen, Z., Thakur, T., Wallach, D. S., & Subramanian, D. (2015). Known unknowns: An analysis of Twitter censorship in Turkey. In *Workshop on Privacy in the Electronic Society*. ACM. https://censorbib.nymity.ch/pdf/Tanash2015a.pdf

Tanash, R., Chen, Z., Wallach, D., & Marschall, M. (2017). The decline of social media censorship and the rise of self-censorship after the 2016 failed Turkish coup. In *Free and Open Communications on the Internet*. Usenix. https://www.usenix.org/system/files/conference/foci17/foci17-paper-tanash.pdf

Teleindustrien. (2021, June). https://www.teleindu.dk/brancheholdninger/blokeringer-pa-nettet

Telekom Control Commission. (2023, January). *Decisions by the regulator on net neutrality*. https://www.rtr.at/TKP/was_wir_tun/telekommunikation/weitere-regulierungsthemen/netzneutralitaet/nn_procedures.en.html

Telekom Control Kommission (TKK). (2023, January). https://www.rtr.at/TKP/wer_wir_sind/tkk/TKK.de.html

The Council of the European Union. (2022, March). *Council regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2022:065:FULL&from=EN

The Gaming Commission—The regulator of the gambling sector in Belgium. (2023, January). https://www.gamingcommission.be/en

The latest crazy law. (2022, April). https://www.revk.uk/2022/04/the-latest-crazy-law.html

The National Authority for Administration and Regulation in Communications (ANCOM). (n.d). *Ancom—Decizii Decret stare de urgenta*. https://www.ancom.ro/decizii-implementare-decret-195-pentru-instaurarea-starii-de-urgen539a_6253

The Public Utilities Commission. (2021, June). *Report on compliance with the regulation of open internet access*. https://ec.europa.eu/newsroom/dae/redirection/document/78862

The Republic of Croatia, Ministry of Finance, Tax Administration—Blocklist. (2021, June). https://www.porezna-uprava.hr/Dokumenti%20razno/Nedozvoljeno%20obavljanje%20djelatnosti%20igara%20na%20sre%C4%87u%20putem%20interneta/Popis%20web%20adresa%20prire%C4%91iva%C4%8Da%20igara%20na%20sre%C4%87u%20za%20koje%20je%20izdan%20nalog%20o%20zabrani%20rada.pdf

UKE przystąpił do porozumienia chroniącego abonentów—Urząd Komunikacji Elektronicznej. (2021, June). https://www.uke.gov.pl/akt/uke-przystapil-do-porozumienia-chroniacego-abonentow,300.html

Urząd Komunikacji Elektronicznej. (2020, June). *Report on compliance in the Polish market with Regulation 2015/2120 on open internet access*. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68330

Ververis, V., Ermakova, T., Isaakidis, M., Basso, S., Fabian, B., & Milan, S. (2021). Understanding Internet censorship in Europe: The case of Spain. In *WebSci '21: 13th ACM Web Science Conference 2021* (pp. 319–328). Association for Computing Machinery. https://doi.org/10.1145/3447535.3462638

Ververis, V., Isaakidis, M., Loizidou, C., & Fabian, B. (2017). Internet censorship capabilities in cyprus: an investigation of online gambling blocklisting. In *E-Democracy*. Springer. https://censorbib.nymity.ch/pdf/Ververis2017a.pdf

Ververis, V., Isaakidis, M., Weber, V., & Fabian, B. (2019). Shedding light on mobile app store censorship. In *Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization, UMAP'19 Adjunct*. ACM. https://dl.acm.org/doi/10.1145/3314183.3324965

Ververis, V., Kargiotakis, G., Filastò, A., Fabian, B., & Alexandros, A. (2015). Understanding Internet censorship policy: the case of Greece. In *Free and Open Communications on the Internet*. Usenix. https://www.usenix.org/system/files/conference/foci15/foci15-paper-ververis-updated-2.pdf

Winter, P., & Lindskog, S. (2012). How the Great Firewall of China is blocking Tor. In *Free and Open Communications on the Internet*. Usenix. https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf

Wright, J. (2012). *Regional variation in Chinese internet filtering* (Tech. rep.). University of Oxford. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2265775_code1448244.pdf?abstractid=2265775&mirid=3

Xu, X., Mao, Z. M., & Halderman, J. A. (2011). Internet censorship in China: Where does the filtering occur? In *Passive and Active Measurement Conference* (pp. 133–142). Springer. https://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf

Yadav, T. K., Sinha, A., Gosain, D., Sharma, P. K., & Chakravarty, S. (2018). Where the light gets in: Analyzing web censorship mechanisms in India. In *Internet Measurement Conference*. ACM. https://delivery.acm.org/10.1145/3280000/3278555/p252-Yadav.pdf

Zittrain, J. L., & Palfrey Jr., G. J. (2007, June). *Access denied: the practice and policy of global internet filtering*. https://www.oii.ox.ac.uk/archive/downloads/publications/RR14.pdf

Zveejovan daje ze Seznamu nepovolench internetovch her k 29.6.2021. (2021, June). https://www.mfcr.cz/cs/soukromy-sektor/hazardni-hry/seznam-nepovolenych-internetovych-her/2021/zverejnovane-udaje-ze-seznamu-nepovoleny-42322

How to cite this article: 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*, 1–28. https://doi.org/10.1002/poi3.367