Understanding Internet Censorship in Europe: The Case of Spain

Vasilis Ververis
Humboldt University of Berlin
Germany
University of Amsterdam
Netherlands

Tatiana Ermakova
Weizenbaum Institute
Fraunhofer FOKUS
Technical University of Berlin
Germany

Marios Isaakidis
University College London
United Kingdom

Simone Basso
Open Observatory of Network Interference (OONI)
Italy

Benjamin Fabian
Weizenbaum Institute
Technical University of Applied Sciences Wildau
Humboldt University of Berlin
Germany

Stefania Milan
University of Amsterdam
Netherlands

ABSTRACT

European Union (EU) member states consider themselves bulwarks of democracy and freedom of speech. However, there is a lack of empirical studies assessing possible violations of these principles in the EU through Internet censorship. This work starts addressing this research gap by investigating Internet censorship in Spain over 2016-2020, including the controversial 2017 Catalan independence referendum. We focus, in particular, on network interference disrupting the regular operation of Internet services or contents.

We analyzed the data collected by the Open Observatory of Network Interference (OONI) network measurement tool. The measurements targeted civil rights defending websites, secure communication tools, extremist political content, and information portals for the Catalan referendum.

Our analysis indicates the existence of advanced network interference techniques that grow in sophistication over time. Internet Service Providers (ISPs) initially introduced information controls for a clearly defined legal scope (i.e., copyright infringement). Our research observed that such information controls had been re-purposed (e.g., to target websites supporting the referendum).

We present evidence of network interference from all the major ISPs in Spain, serving 91% of mobile and 98% of broadband users and several governmental and law enforcement authorities. In these measurements, we detected 16 unique blockpages, 2 Deep Packet Inspection (DPI) vendors, and 78 blocked websites.

We also contribute an enhanced domain testing methodology to detect certain kinds of Transport Layer Security (TLS) blocking that OONI could not initially detect. In light of our experience analyzing this dataset, we also make suggestions on improving the collection of evidence of network interference.

WebSci '21, June 21–25, 2021, Virtual Event, United Kingdom

ACM ISBN 978-1-4503-8330-1/21/06.
https://doi.org/10.1145/3447535.3462638

ACM Reference Format:
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 (WebSci '21), June 21–25, 2021, Virtual Event, United Kingdom.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3447535.3462638

1 INTRODUCTION

Surveillance and network interference infrastructures are increasingly deployed in EU member states to contain content and services that do not comply with EU legislation [7], e.g., online gambling, copyrighted material, incitement to the commission of crimes, depictions of cruel violence against humans, human death or mortal suffering, child or animal exploitation material [49]. However, despite the presumably tacit assumption that illiberal practices in the digital realm are rather likely to affect only authoritarian states, EU member states also gain attention with respect to incidence and modalities of Internet censorship [14, 45, 46, 55, 56]. Moreover, instances of "everyday acts of authoritarianism" online could be observed also in the democratic West, often with industry-state collaboration and no democratic oversight [25]. To this end, we define online censorship as any form of network interference that disrupts the normal operation of services or content in the World Wide Web to prohibit access to a specific audience. Previous research examined the presence of censorship in various countries such as China [19, 31], Thailand [23], Bangladesh [33], Pakistan [1, 34], India [24, 57], Iran [5, 9], Syria [4, 15], Turkey [50, 51], Russia [44], and Mexico [28]. There is almost no previous research about the topic of censorship in Spain, except for some clues [3, 6, 11, 29, 40]. Lundström and Xynou [29] observed that 25 sites related to the 2017 Catalan independence referendum were blocked from September 25 up to the day of the referendum (October the 1st), utilizing DNS manipulation and HTTP blocking, based on the Open Observatory of Network Interference (OONI) network measurements data retrieved from three local networks. A technical report by Ververis et al. [54] provides an analysis on persistent blocking of the Women on Web (WoW) website by all major ISPs in Spain from network measurements of the first quarter in 2020.

Referring to the lack of similar studies and seeking to fill the identified research gap, this article examines the practice of Internet censorship in Spain. Motivated by partial insights [3, 6, 11, 29, 32,

40, 54] and based on historical network measurements provided by the data of OONI [38], our research observes fours years (July 2016 to May 2020), including October 2017, where the Spanish referendum on Catalonia independence took place. The referendum was called by the Catalan authorities, but declared unconstitutional and suspended by the Spanish government. Held amidst repression and violence by the central government, it asked Catalan citizens: *"Do you want Catalonia to become an independent state in the form of a republic?"* The *"yes"* won with over 92 percent of popular vote [40]. Due to its highly controversial nature, the referendum represents an excellent case to observe online censorship in action. We set 2016 as the starting year for our analysis due to higher availability of OONI data. We address the following research questions:

- Which network interference techniques were in place in Spain over the past four years?
- How did the techniques evolve during the investigated time period?
- How can such an Internet censorship study be reproduced, and our method generalized to other cases?
- What are the limitations of such a long-term historical data analysis and how can we improve the measurement collection and analysis methodology?

The paper is organized as follows: Section 2 provides the methodology for choosing a data source, processing and validating the network measurement data used in this study, categorizing websites into categories. Then, Section 3 proceeds with analyzing the data and reports our findings of network blocking via HTTP blocking, DPI, DNS Manipulation, domain seizure, the case of WoW website blocking, Server Name Indication (SNI) blocking, and TLS interception, with the improvement of TLS interception testing methodology in OONI, followed by the circumvention of DPI blocking and the reproducibility of our research. Finally, the general contributions of our study and implications for research and practice are discussed in Section 4, followed by the ethical considerations in Section 4.2 and our conclusions in Section 5.

2 METHODOLOGY

We begin by introducing our methodology. This consists of four main parts: (i) choice of an appropriate data source; (ii) processing and (iii) validation of network measurement data; (iv) clustering websites into categories; (v) data analysis.

2.1 Data sources

We surveyed several tools that perform network measurements to detect Internet blocking and provide a repository of historical data, with a special focus on residential endpoints [2, 10, 35, 38, 42]. Specifically, we considered IClab [35], Censored Planet [42], RIPE Atlas [10] and OONI [38]. IClab mainly uses VPN endpoints for its network measurements [35]. Censored Planet tests scan the IP address space for accessible public servers excluding end-user devices and target servers, routers or embedded devices [52] and therefore do not cover residential ISP networks. RIPE Atlas is not designed to measure Internet censorship and thus HTTP measurements are not allowed to run on residential ISPs [10]. Albeit one could infer useful information by performing other available tests on residential ISPs that block websites. We abstained from using RIPE Atlas probes due to the ethical considerations and the inaccessibility of Internet blocking methodologies. Nonetheless, we queried all evaluated data repositories for any historical network measurements that could match our study's requirements. We did not find any matching data that apply to our research. Out of all the evaluated tools, only OONI provides longitudinal data of historical network measurements for our desired period (years of 2016 to 2020). We found the OONI data repository provides adequate data of over 3 million network measurements from all major residential ISPs in Spain over the last 4 years. Nevertheless and as with any software, OONI Probe software has some limitations in their TLS blocking test methodology, as we found during our data analysis. We present detailed explanations on how we overcome this limitation and implement a new testing methodology, which has been approved by the OONI developers, and is now in further development for wider adoption to the public (see Section 3.7). All software components of OONI's source code are released under a free and non-restrictive license and are available for everyone to download, modify and use.

2.2 Data processing

OONI has been collecting network measurements from anonymous volunteers since 2012 [38] to detect evidence of possible network interference that might relate to Internet censorship or surveillance on different vantage points, primarily from anonymous end-hosts in residential networks. OONI data is made available under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International license and could thus be used freely and without restrictions in our research study. We chose as the blocking methodology test the Web Connectivity test [37], that measures the reachability and possible blocking of any website, given an IP address or domain name. The test consists of the following steps: i. Performing A and AAAA DNS lookups and storing the result of the A records list, ii. Attempting to establish a TCP session on either port 80 or 443 (depending on the URI scheme), and iii. Performing an HTTP GET request to the path specified in the URI. In all steps, the responses and possible errors are recorded in a JSON file and submitted to the OONI network measurements collector for further processing and archiving [37].

To get access to the OONI data, one may use the OONI API and OONI Explorer. However, both tools have some limitations regarding the file size of the measurements and the computational time required to get a vast amount of data. To overcome these limitations and not stress the OONI services, we setup a PostgreSQL replica of the OONI meta database. Next, we fetched the latest archived data required for a database cluster (PGDATA). 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). It took about 10 days to sync with the master database and 800 GiB of storage capacity to accommodate the OONI meta database. The main requirement of a replica is a system with enough storage capacity and network connectivity to host a PostgreSQL database. Once the meta database was synced, we were able to run queries based on our blocking methodology heuristics and the criteria set to eliminate potential false positives. We used self-developed IPython notebooks (see Section 3.10) to query the database for our study data and process the retrieved data, whereas we used heuristics

(see Section 2.4) to validate the correctness of data and ensure that there are no false positives or negatives. Here, we also categorized the data for further processing. Next, we used the R programming language to plot graphs. Finally, all the data were summarized and exported in CSV files for easier sharing and reproducibility.

2.3 Blockpage similarity heuristics

Based on the discovered blocked websites we built heuristics that reveal evidence of network interference. We used the simhash [30] technique to estimate the HTML body text and length of blockpage fingerprints found, allowing us to detect further blockpage fingerprints. The ISP blockpages are typically based on static pages as they are easier to configure and less computationally demanding in comparison to the dynamic blockpages. However, dynamic blockpages include more information, such as tracking bits, that can be used by customer support or other entities within an ISP for statistical purposes or legal regulation. The SHA256 checksum of the HTML body can be reliably used as a fingerprint to identify static blockpages triggered by other websites. In the case of dynamic blockpages, the low hamming distance between the blockpage and the HTML body simhash was used to reliably discover further fingerprints and identify new blocked websites. This applies to the OONI meta database columns *body_simhash* and *body_text_simhash*. Due to the vast amount of data, we built more than a hundred fingerprints, first to eliminate any false positives, subsequently to detect new blockpages, and finally to enumerate all blocked websites. Additionally, to be confident that our methodology was correct, we manually inspected each of the detected blockpage fingerprints to eliminate any potential remaining false positives. As we created more fingerprints, we iterated our data validation process until no more false positives were left in our dataset. For the qualifying blocked websites, we defined a set of requirements and criteria, described in Section 2.4.

2.4 Data validation

Despite the presence of multiple network measurements with signs of network interference, we included only those blockpages or instances of blocking that could be verified with certainty, i.e., neither being false positives (for instance due to network connectivity errors) nor blocked due to internal network filtering regulations (such as parental controls, antivirus filtering or firewalls). Specifically, we considered only network measurements that suffice the following heuristics:

- Existence of a blockpage or any indication of blocking error (i.e. HTTP status code 403);
- Existence of DNS records that point to bogon IP addresses (such as 127.0.0.1);
- Removal of network measurements with wrong autonomous system (AS) information (i.e. AS0);
- No blocking based on internal network filtering infrastructure (parental controls, firewall, antivirus, proxies);
- No blocking based on CDN or webserver specific filtering or security products (such as Cloudflare, Sucuri, Incapsula, Zscaler).

Due to ethical considerations, we excluded from our analysis those network measurements that may violate the anonymity of the person/entity who submitted them. We reported possible personally identifiable information in network measurements to the relevant software entities responsible for collecting these data.

Civil Rights & Political	Sci-Hub	Democratic Tsunami	Referendum	Copyright
womenonweb.org	sci-hub.se	api.tsdem.org	alerta.cat	digitalplatinum.in
eln-voces.com	sci-hub.tw	app.tsdem.org	aniol.github.io	c14.xtra7.gq
		app.tsunamidemocratic.cat	cat.referendum.barcelona	digitalservices.tel
		app.tsunamidemocratic.com	garantiespelreferendum.com	elitegol.global
		democratictsunami.eu	nigeon.github.io	elitegol.tv
		tsdem.org	pedrosanchez.cat	elitegoles.com
		tsunamidemocratic.cat	ref1oct.cat	elitegoltv.me
		tsunamidemocratic.com	ref1oct.eu	elitegoltv.org
		tsunamidemocratic.github.io	ref1oct.net	futbolpirlotv.net
		tsunamidemocratic.net	ref1oct.org	gtmservices.org
			referendum.enricpineda.cat	hightquality.org
			referendum.fun	intergoles.me
			referendum.fyi	intergoles.net
			referendum.legal	iptvadur.eu
			referendum.lol	iptvesp.eu
			referendum.love	iptvld.paranosotros.ru
			referendum.ninja	iptvtool.es
			referendum.observer	landiptv.live
			referendum.party	locopelis.com
			referendum.pau.fm	mamahd.org
			referendum.pirata.cat	movspain.com
			referendum.rip	pandorapremium.ddns.net
			referendum.soy	playlist.topcam.net
			referendum.voto	pirlotv.es
			referendum.works	pirlotvhd.net
			referendum.zalo.nyc	pirlotvhd.online
			referendumcat.eu	pirlotvonline.net
			referendum.cat	playlist.topcam.me
			gateway.ipfs.io	qualitypremium.sytes.net
				realstreaming.net
				redstreamsport.online
				rojadirectaenvivo.es
				sansat.net
				sendspace.com
				todocvd.com
				thepiratebay.org
				thepiratebay.se
				veopartidos.online
				wolftm.in

Table 1: Blocked websites by category type

2.5 Website categorization

Based on the finding of our data analysis, we grouped the blocked websites into five categories, regarding their content and purpose as follows:

i. **Civil Rights and Political**: This category was reserved for the websites of WoW (*womenonweb.org*) and *eln-voces.com*
ii. **Sci-Hub**: Here we included the website mirrors of Sci-Hub, a file-sharing repository of research papers and books;
iii. **Democratic Tsunami**: This category involves websites related to the Catalan protest group Tsunami Democràtic (in English, Democratic Tsunami);
iv. **Referendum Websites**: We reserved this category for websites dealing with the Catalan referendum in 2017;
v. **Copyright Websites**: Here we included websites being blocked on grounds of copyright infringement such as video streaming, IPTV, online indexing of magnet links and torrent files.

The complete list of all the blocked websites by category type is listed in Table 1.

3 ANALYSIS OF NETWORK BLOCKING

In this section, we analyze end-host measurements of network interference in Spain over the last 4 years (from 2016 to 2020) to spot instances of blocking and information controls, the network interference techniques being in place, and the extent of their usage. In total, we process over 3 million network measurements (3,089,892) from 17 different ASes that correspond to ISPs covering 98.45% of all broadband and 90.94% of all mobile subscribers in Spain [18].

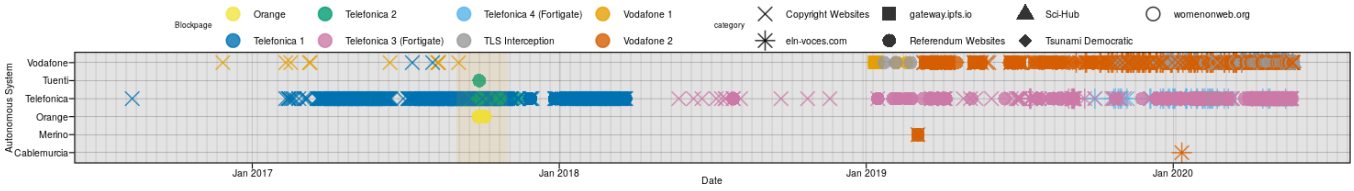

Figure 1: HTTP Blocking of ISP/Date per website category of OONI data in Spain

Although much of the blocking is related to the Catalan referendum, the blocking is not limited to the autonomous community of Catalonia, but is experienced by users in all parts of Spain. The date range of network measurements during the referendum is highlighted with a color overlay visible in Figures 1, 2 and 3. We partition our data analysis into different sections, according to the type of network blocking methodology detected in Spanish ISPs; The list of AS network names, as well as the numbers and the dates of AS registration allocation are listed in [53].

3.1 HTTP Blocking

The first case of HTTP blocking in the network measurements of OONI data from Spain was identified on the 8th of November 2016 with the blocking of the URL *thepiratebay.org*. The website was found systematically blocked under the ISP Telefonica (AS3352). The ISP didn't present any reasons for the blocking, which is a common practice when a website is blocked by an ISP despite the lack of transparency. Instead, users received the *ERROR 404 - File not found* error message that falsely indicates a website error [53]. The relevant measurements of this blockpage are illustrated in Figure 1 under the group name *Telefonica 1*. Later on, on the 26th of November 2016, we see the same URL being blocked for the first time within the Vodafone ISP (AS12430 and AS6739). In this blocking instance, users were redirected with the HTML meta refresh method (*http-equiv="refresh"*) to the blockpage URL *http://castor.vodafone.es/public/stoppages/stop.htmopt* [53]. This blockpage is represented as *Vodafone 1*, in Figure 1. Subsequently, after the 11th of May 2017, the same URL was found being blocked with a different blockpage in Telefonica. However, the string `PHISHING_TSOL_MENSAJE_1` in the HTML source code may indicate the Telefonica Solutions group (TSOL) could be using the same blockpage to filter phishing websites [22]. Additionally, on the source code of that blockpage, we found the name of another authority (in Spanish) *Administrativo Ley del Juego* redirecting users elsewhere to the IP address of the (blockpage) *http://195.235.52.40* [53]. An indication that the blockpage may be used to block other websites. In Figure 1, this blockpage is tagged as *Telefonica 2*.

3.1.1 Information controls of Catalan Referendum. We identified 24 unique blocked URLs including the InterPlanetary File System (IPFS) gateway, a peer-to-peer network for storing and sharing data over a distributed filesystem. The categories of websites blocked during that period were copyright and referendum websites. The complete list of the blocked URLs can be found in Table 1. Furthermore, we identified seven new blockpages that contained information related to the referendum, including the names of the authorities under which the websites are blocked and which changed in later versions of the blocking from `PHISHING_TSOL_MENSAJE_1` to `Judicial_Policia_Nacional`.

3.1.2 Javascript switch statement for different blocking rules. The HTML body of the blockage [53] tagged in Figure 1 as *Telefonica 3 (Fortigate)* indicates that Telefonica may block more websites. In the code section, a switch statement evaluates the name expression, that matches the value to the case clause. In this blockpage, there are four different cases that set the HTML *h1* heading element or redirect to a URL, specified by the *replace()* method of the location interface. Specifically, the first case `PHISHING_TSOL_MENSAJE_1` sets the heading to *Error de acceso por contenido no identificado* (translated from Spanish to *Access error due to unidentified content*). The second case clause sets the heading of the page to `Administrativo_Ley_del_Juego` and redirects users to the blockpage hosted in Telefonica's network at *http://195.235.52.40*. The third case clause used by Guardia Civil sets the heading of the page to `Judicial_Guardia_Civil` and redirects the user to *http://paginaintervenida.edgesuite.net* when triggered by a blocked website related to the Catalan referendum. This blockpage is hosted in Akamai's network. Last, the default case (*id="causa"*) corresponds to the blockpage of *http://thepiratebay.org* which sets the heading of the page to *ERROR 404 - File/block not found* and which redirects users to the URL *http://webbloqueadaporpolicianacional.com*.

When further examining the blockpage's source code, we identified the URL of `Judicial_Guardia_Civil`, redirecting users to the URL *http://www.marca.com*, a Spanish national sports website owned by the company Unidad Editoria. We observed that information regarding the blocking was rather minimal or non-existent, e.g., given by an error code message at a website (HTTP 404). All source codes of the blockpages found to trigger this blocking technique (Javascript switch statements) are listed in [53]. One variation of the blockpage is illustrated in Listing 1.

Orange ISP was found to censor websites via HTTP blocking only during the period of the Catalan referendum. Later on, Orange switched to blocking websites via means of DNS manipulation. This finding probably suggests that Orange ISP used a different type of network blocking for censoring websites related to information on the Catalan referendum. Specifically, Orange ISP presented to users a blockpage with the exact source code used in URL *http://paginaintervenida.edgesuite.net*, however, Orange didn't redirect its users to the blockpage but rather used HTTP blocking to block access to the websites in question. The relevant measurements are grouped under the shape *Orange* as illustrated in Figure 1.

We proceed with studying detected blocking instances after the referendum period up to the end of our data analysis (2017-11-01

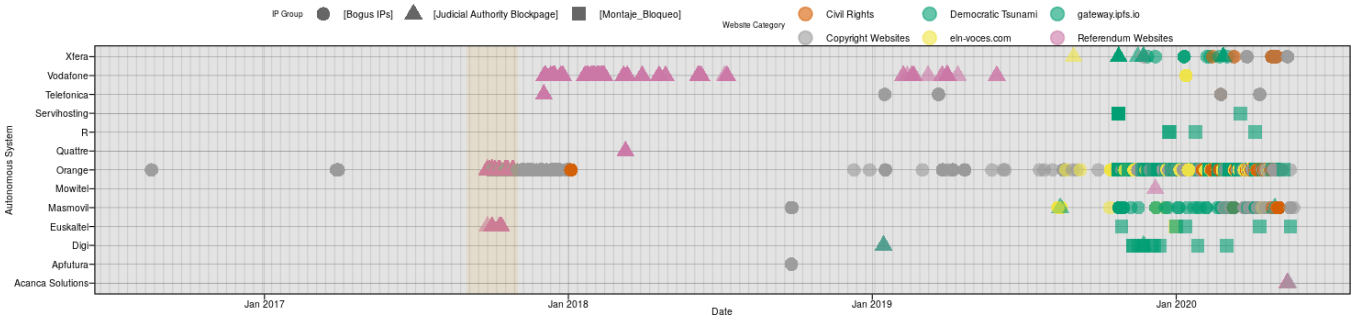

Figure 2: DNS Manipulation of ISP/Date per website category and IP group of OONI data in Spain. For an expanded version of this figure with layers per Website category and AS see Figure 3

to 2020-05-21). In Vodafone networks, we identified two additional distinct blockpages. The first [53] was deployed to block a few referendum websites and the IPFS gateway, whereas the second blockpage [53] was extensively used for other website categories such as websites related to copyright, referendum (including the IPFS gateway), as well as civil and political websites. As in previous years, Telefonica ISP censored websites without any explanation of the reason for the blocking in contrast to other ISPs. Based on the network measurements, we extracted 21 different blockpage variations grouped in 4 different blockpage tags (*Telefonica 1* to *Telefonica 4*) per website category, as illustrated in Figure 1.

3.2 Deep Packet Inspection

Several blockpages that were found in network measurements of Telefonica confirmed the existence and usage of the DPI equipment vendor Fortinet [20]. Specifically, the blockpages with sizes of 332 to 339 bytes exposed several configuration settings of Fortinet's Fortigate DPI equipment used by Telefonica ISP [53]. The difference of 7 bytes between the blockpages is due to the different configuration options of hostnames and IPs. From the comments section revealed in the HTML source code of the blockpage, the settings of the Fortigate device can be ascertained as: *CATEGORY* for the web filter category (if any), *DEST_IP* for the destination IP of the blocked resource, *SOURCE_IP* for the source IP of the request (the source IP of the user) and the *FGT_HOSTNAME* that reveals the hostname of the Fortigate device. According to the documentation of Fortinet, the aforementioned variables (except the category variable) are used as replacement messages for the web filtering, thus the variable will change dynamically depending on the user's IP, targeted websites, and Fortigate device's hostname [21]. The *SOURCE_IP* variable is masked with the word [REDACTED]; this is done by the OONI software to protect the privacy of the users and not leak any personally identifiable information.

Further blockpages found under the Telefonica networks with sizes of 1290 and 1292 bytes reveal more configuration settings of the Fortigate devices. They expose (among other settings) the *POLICY_UUID*, which is the universal unique identifier (UUID) for the policy in Fortigate's configuration. The complete blockpage with byte size 1290 [53] is illustrated in Figure 1 with the tag *Telefonica 3 (Fortigate)*. Few measurements from Telefonica found in this period reveal blockpages with sizes of 1514 and 1517 bytes deployed only during the referendum period, until mid January 2018 [53]. These blockpages are illustrated in Figure 1 under the tag *Telefonica 2*. Finally, the last blockpages identified in Telefonica target exclusively the URL *http://www.eln-voces.com/*. In this case, we see a variation of previous blockpages analysed in this section with the addition of one more entity listed as a switch case (analyzed in Section 3.1.2) in blockpage's source code, `Direccion_General_de_la_Policia` redirecting users (location replace in Javascript) to the URL *http://a.policia.es/?url=www.eln-voces.com/*. However, the category name on Fortigate's device configuration and the HTML title are set to `Judicial_Guardia_Civil` and not to the `Direccion_General_de_la_Policia` as the URL suggests, perhaps due to human error or misconfiguration. These blockpages have a size of 1989 [53] and 2186 bytes. Another finding of the blockpages with size of 2374 and 2377 bytes used in this period reveals two more cases used to block websites in Spain; `PETICION_JUDICIAL_140120` and `Administrativo_Ley_del_Juego_Temporal` both redirecting users to different URLs [53]. The blockpages are grouped under the tag *Telefonica 4 (Fortigate)* illustrated in Figure 1.

3.3 DNS Manipulation

The first identified network measurement that revealed DNS manipulation was detected for the domain name *thepiratebay.org* in Orange ISP (AS12479) on date 2016-08-18 and later for the domain *thepiratebay.se*. In all measurements that displayed signs of DNS manipulation in this era, we found that the A record of the domain names in question pointed to the bogon IP address *127.0.0.1*, commonly reserved for use as the Internet host loopback address (localhost). IPv4 network standards reserve *127.0.0.1* for loopback purposes (and the complete /8 IP address block) must not appear in any network on the Internet (RFC 1700) [41]. The results are illustrated in Figure 2 under the point shape name *Bogon IPs*. Furthermore, we identified 24 unique blocked domains, including the IPFS gateway (*gateway.ipfs.io*) as well as 2 GitHub pages (*aniol.github.io* and *nigeon.gihub.io*) being consistently blocked during the period of the referendum (in October 2017). The blocking of the GitHub pages is evident only via DNS manipulation because of the collateral damage the HTTP blocking of GitHub could have caused (i.e. HTTP blocking would result in the complete blocking of GitHub

website whereas now only specific pages of users are being targeted). This is not the case though for the IPFS gateway that is blocked employing DNS manipulation and also via HTTP blocking.

After the referendum period, new websites are still blocked on the remaining categories: copyright, Democratic Tsunami, Sci-Hub, civil rights, and political in the networks of Orange, Masmovil, Telefonica, and Vodafone ISPs. Apart from censorship of websites for copyright reasons, information controls of the referendum and attempts to silence protests from Democratic Tsunami, we found another case of political censorship concerning the website *eln-voces.com*. In the absence of any further information, we assume that the specified website was blocked because of the content from the terrorist organization National Liberation Army, as defined by the European Union council decision 2017/1426 [16]. From historical DNS data and snapshots from Wayback Machine of Internet Archive, the domain name *eln-voces.com* was expired from 2019-06-12 to 2019-08-25 and then registered by a different hosting entity with unrelated content [8]. Moreover, we found that the website *womenonweb.org*, a non-profit organization providing support to women, was blocked since 2020-01-30 and until the completion of our research (2020-05-21). The website is blocked in ISPs Orange, Masmovil, Telefonica, and Vodafone. See Section 3.5 for a detailed analysis of this blocking. All domain names blocked via means of DNS manipulation are listed in Table 1. Figure 1 illustrates the website category blocked and under which blockpage (IP group).

3.4 Domains Seizure

The domains *alerta.cat*, *ref1oct.cat* and *referendum.cat* were seized and their DNS records pointed to a website hosted under the Akamai Technologies CDN network (*edgesuite.net*) with the logo of the Spanish judicial authority and the following text: *This domain name has been seized according to a seizure warrant under the Judicial Authority and is under its administration.* The website *paginaintervenida.edgesuite.net* was still accessible as to the time of this research. However, we found the aforementioned domains blocked in specific networks via means of DNS manipulation or HTTP blocking. The domains *referendum.clash.cat*, *marianorajoy.clash.cat* and *marianorajoy.cat* were not blocked but were instead seized by the Spanish Judicial Authority.

3.5 Blocking of Women On Web

Our data analysis revealed the persistent blocking of the WoW website by all major Spanish ISPs. OONI network measurements indicate that most Spanish ISPs had been blocking the WoW website since the end of January 2020. The blocking methodologies are similar to the other blocked websites as determined in our data analysis: DNS manipulation and HTTP blocking using DPI infrastructure. Our data analysis and reports from volunteers indicate that the following ISPs blocked the WoW website: Vodafone, Orange, Masmovil, Xfera, and Telefonica. Table 2 summarizes the blocking methodology as well as the DPI technology (when applicable) deployed per ISP.

Measurements from Vodafone (AS6739) show another blocking strategy, consistently over time, suggesting that between 16/03/2020 and 24/04/2020, Vodafone moved from a simpler to a more complex blocking strategy. Additionally, the identified DPI products analyzed in Section 3.2 are both used to block access to WoW: Fortinet in Telefonica's network and Allot in Vodafone's network. In January 2021, WoW filed a lawsuit at the Spanish National Court for the illegal and unjustified blocking of their website [36].

ISP	Blocking Technique	DPI
Telefonica	DNS Manipulation, HTTP Blocking	Fortinet
Vodafone	HTTP Blocking, TLS Interception	Allot
Orange	DNS Manipulation	-
Masmovil	DNS Manipulation	-

Table 2: Women On Web website blocking techniques per ISP

3.6 SNI blocking

Another technique detected in Vodafone networks is SNI blocking. SNI is a TLS extension used in webservers that host multiple websites reachable under HTTPS on the same server. The SNI attribute is transmitted in clear text and provides the website's hostname in question, thus making it easy to block. TLS protocol (version 1.3) adds experimental support for SNI encryption. However, as TLSv1.3 is a relatively new protocol and given that SNI encryption is still experimental, it may take some time to get widely deployed. As of the latest estimations, deployment of TLSv1.3 on popular domains is about 30%, and 10% across the com/net/org top-level domains [26]. In Section 3.7, we present further details on our TLS interception findings during our data analysis that also apply to the case of the WoW website blocking.

3.7 TLS interception

We discovered several measurements that present a certificate verification failure in Vodafone networks (AS12357, AS12430, and AS6739). The error (`ssl_error:error:14007086:SSLroutines:CONNECT_CR_CERT:certificate verify failed`) indicates that there could be TLS interception on the network. This error message from the OpenSSL library indicates that the TLS handshake is over, and the client cannot verify the certificate provided by the server. OONI's current test methodology does not capture any further details related to TLS interception. Thus, we performed further tests using the OpenSSL command-line tool. We discovered that we were connecting to a box serving a forged, invalid TLS certificate claiming to be the blocked website. This box was the same one hosting the Vodafone blockpage [53]. All websites or categories blocked utilizing TLS interception are illustrated in Figure 1.

3.8 Improvement of TLS interception testing methodology

We used the results collected by OONI's Web Connectivity experiment [37]. This experiment implements the following algorithm. It takes in input a website's URL (either using HTTP or HTTPS). It resolves the website's domain name using the system DNS resolver. Then, it attempts to connect to every resolved IP address. Next, it

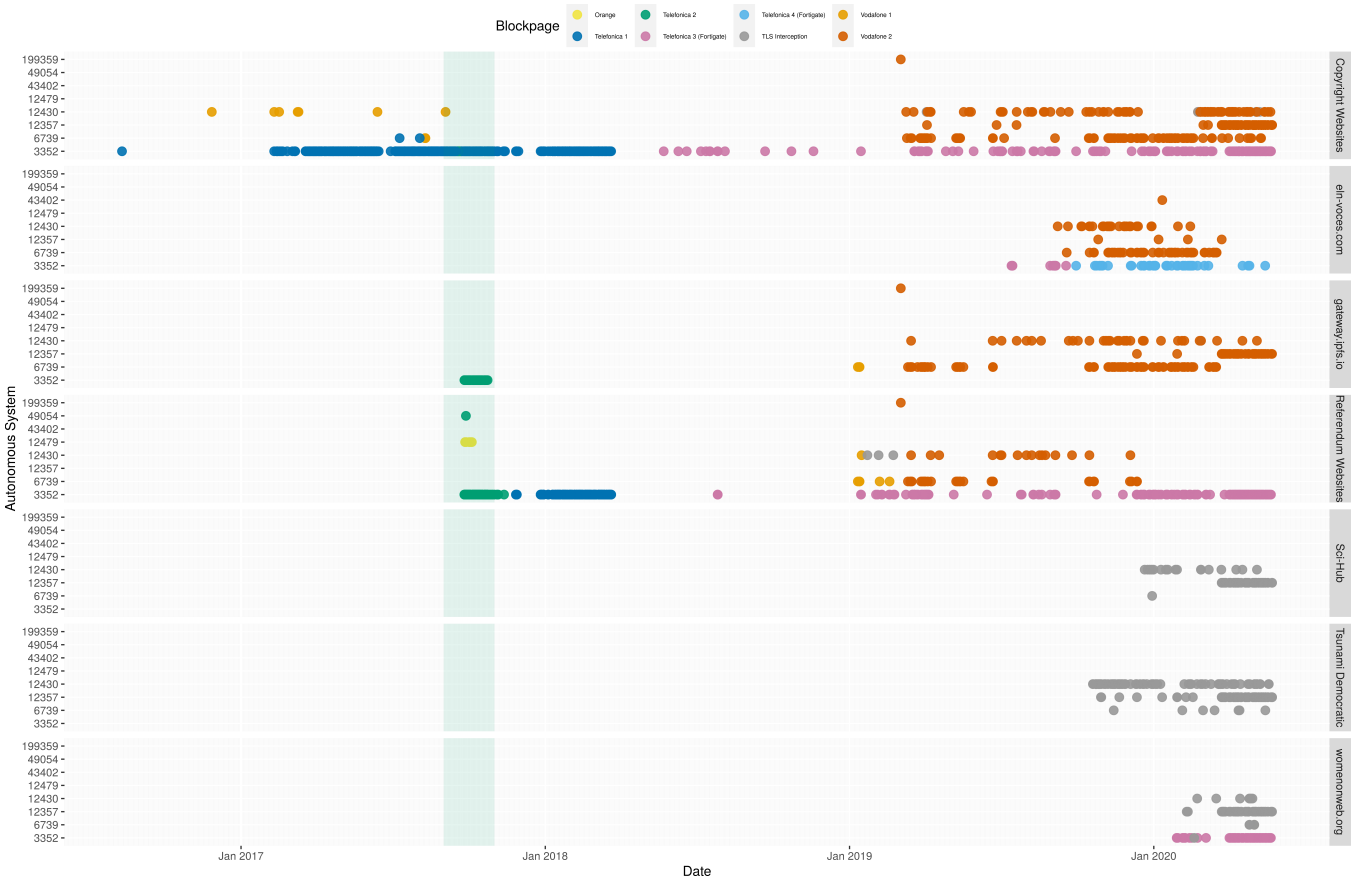

Figure 3: DNS Manipulation of AS/Date per website category (in layers) and IP group of OONI data in Spain

tries to fetch the website's URL. Finally, OONI compares its measurement results with a concurrent measurement performed by a test-helper server to detect false positives.

3.8.1 Issues with OONI's Web Connectivity. In the context of WoW TLS blocking, the main issue of OONI's Web Connectivity methodology is that it did not collect enough low-level information around the TLS connection. To overcome this limitation, we implemented Aladdin, a ten-step network experiment based on the OONI measurement engine that significantly extended the Web Connectivity methodology [12] to characterize the WoW censorship case.

3.8.2 Description of Aladdin. The input of Aladdin is a website's domain name. Aladdin assumes that the website is available over both HTTP and HTTPS. These are the Aladdin's steps:

The first step checks whether there is SNI-based blocking. We connect to an unrelated server (e.g., example.com:443) using the SNI of the target website (e.g., blocked.com) and an unrelated SNI (e.g., ok.com). If only the connection using the target website SNI is blocked, we conclude that there is probably SNI-based blocking.

The second step checks whether there is Host-header-based blocking. We connect to an unrelated server (e.g., example.com:80) using the Host header of the target website (e.g., blocked.com) and an unrelated Host header (e.g., ok.com). If only the connection using the target website Host header is blocked, we conclude that there is probably Host-header-based blocking.

The third step checks whether there is DNS injection. It sends a DNS query to a host that we know is running no DNS server. If we get back a reply, then there is DNS injection.

The fourth step queries the default resolver (like Web Connectivity does). In addition to recording the returned addresses, this step notes whether any of them is a private address (e.g., 10.0.0.1).

The fifth step repeats the DNS query using Google's DNS over HTTPS (DoH) server. Then it checks whether the IPs returned by the default resolver are consistent with the ones returned via DoH.

The sixth step fetches the webpage over HTTPS using the IP addresses returned by the system resolver. Suppose an IP address returned by the system resolver is invalid for the domain (i.e., suppose it is a private address or just the address of an unrelated server). In that case, this step will fail because TLS would not be able to map the returned certificate to the requested domain.

The seventh step fetches the webpage using the Psiphon circumvention tool. We compare the webpage fetched using Psiphon to the one fetched in the sixth step. This step is similar to what Web Connectivity does, except that we are using the Psiphon circumvention tool instead of the test helper.

The eighth step disables TLS certificate validation and then fetches the webpage again. This step allows collecting the returned certificate and possibly fingerprinting the blocking device.

The ninth step repeats the sixth step, except that it uses the IP addresses returned by the DoH resolver.

The tenth step is like the ninth step, except that we explicitly force the code to use TLSv1.3. In TLSv1.3, the server's certificate is encrypted. This fact gives us confidence that blocking depends on the cleartext content in the Client Hello (typically, the SNI).

3.8.3 Findings. After repeatedly running the Aladdin experiment for WoW, we discovered the following: (1) there was no SNI-based blocking (step 1); (2) following the IP address returned by the system resolver leads to a TLS verification error (step 6); (3) disabling TLS certificate verification allows us to fetch a certificate signed by Allot (step 8); (4) the IP address returned using DoH (step 5) is the same returned by the system resolver (step 4) and used in step 6 (i.e., `67.213.76.19`). We thus confirm TLS interception of the WoW website possibly using technology developed by Allot.

3.9 Circumventing DPI blocking

We were able to circumvent the DPI blocking by adding the tab escape character (*\t*) to the basic HTTP get request headers. Another technique to circumvent the DPI blocking is by delaying the transmission of the HTTP get requests, as mentioned in [22] where they circumvented DPI blocking websites with information related to the Catalan referendum in 2017. This is another indication that the ISPs are using the same blocking infrastructure throughout periods for blocking of different content and by different authorities.

3.10 Reproducibility

Our research is reproducible and can be replicated to obtain our dataset and results. All parts of our data analysis including the heuristics used to analyse the network measurements as well as the source code developed during our experimental testing methodology to overcome previous limitations of OONI Probe's software as well as the OONI meta database is made publicly available and online under a free and open source software license [13, 53].

4 DISCUSSION

In this research, we observed that the websites related to the controversial Catalan referendum were blocked with the common blocking techniques. We were able to detect 16 unique blockpages, identify 2 DPI vendors (Fortigate and Allot) and a total of 78 websites being blocked. For an overview of the blocked websites and reproducibility, we compiled a matrix of all the blocked websites in Table 1. To the best of our knowledge, this is the only empirical study that provides a complete list of blocked websites in Spain. None of the blockpages contained any information on a law order or blocking reasons. Spanish authorities and ISPs appear to rather obfuscate the blocking information through misconfiguration of the blockpages as if the websites were not blocked but rather unreachable or erroneous. Nevertheless, being transparent about the blocked websites, also by issuing blocklists, may help to reduce over-blocking, unintended blocking or collateral damage [56] such as the blocking of an expired domain name registered from a different entity. Starting from the date 2017-09-25, we found an increase of network measurements in OONI data. The ISPs might have been preparing to block all websites related to the Catalan referendum. [29, 40] report that the Spanish court deemed the Catalan referendum of October the 1st 2017 illegal and the Spanish government attempted to stop the referendum voting by blocking access to websites, raiding the offices of the .cat Internet registrar, seizing domain name sources, and removing an application from Google Play Store. [29] also identified DNS manipulation and HTTP blocking predominantly used to censor Catalan referendum sites.

In line with these findings, we revealed the same websites in the non-DNS analysis, with more blocked websites for file sharing, video streaming, IPTV links, the gateway of IPFS (*gateway.ipfs.io*), WoW website (*womenonweb.org*) and the ex-website of the National Liberation Army in Colombia (*eln-voces.com*) that expired almost a year ago and then was registered by another entity [8, 47] hosting unrelated content. We additionally detected multiple middleboxes (DPIs) also used to block access to websites. Prior research by the Opennet Initiave in 2005 identified Burma's (Myanmar's) repressive regime to use Fortinet's Fortiguard product for censorship and information controls of websites and services in Burma's ISP networks [27] — similarly to Telefonica ISP for blocking numerous websites in Spain, as analysed in Section 3. In analyzing past events, our study is limited by the historical OONI network measurement data. More accurate measurements and cross-correlations could be potentially achieved by combining with other data sources, however, all data sources evaluated in Section 2.1 did not have relevant network measurements available that could match our research requirements (see Sections 1 and 2.4). It is also worthwhile acknowledging that our manual checks to ensure that there are no false positives might have resulted in removing some blocked websites from the data set. Although the stated limitations did not prevent us from addressing our purpose, we leave these issues to future work. Compared to other network measurement studies on a larger amount of countries in their network interference practices [35, 39, 43, 52], this present study enabled deeper technical insights in the stated field. Further, our study demonstrated the possibility of feasible, effective, and verifiable research and conclusive results based on historical network measurement data.

4.1 Involvement of multiple authorities

Cascading censorship and blocking that involves different stakeholders illustrate how power dynamics form a hierarchy within the sphere of control of a nation-state authority. In our research, we identified numerous entities that can force ISPs to block access to Internet resources and perform information controls. The Spanish Civil Guard (Guardia Civil), the General Directorate of Police (Direccion General de la Policia), Judicial National Police (Judicial Policia Nacional), Gambling Authority (Dirección General de Ordenación del Juego). Furthermore, the anti-phishing security group of Telefonica Solutions (TSOL) seems to also be able to decide which websites or services can be blocked, as discussed in Section 3.1.1.

4.2 Ethical Considerations

In our research, we used only free software tools and datasets available under a free license (Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International). We neither conducted nor asked any entities to perform network measurements. The data collected by OONI probes was sanitized to remove any personally identifiable information. The OONI team provides all data specifications and methodologies as well as the source code of their software.

5 CONCLUSION

This study analyzes OONI historical network measurements in Spain in the 2016-2020 period. We provide strong evidence that the Spanish network blocking infrastructure originally introduced for enforcing copyright and gambling regulations was also used to control political information. We documented the blocking of several websites and services, including those related to the Catalan referendum. The website of the Catalan protest group Democratic Tsunami was also blocked. We also measured the blocking of a non-profit organization's website providing support to women, Women on Web. We additionally found that a previously expired domain name now registered under a new entity (*eln-voces.com*) was also blocked. Furthermore, we detected and listed all network interference techniques deployed by the Spanish ISPs, which included DNS manipulation and HTTP blocking with DPI equipment. We ascertain that both blocking techniques were consistently used by each ISP, at the same time in some cases not being labeled as such in a transparent way. Our research highlighted the importance of systematic, longitudinal network measurements in a geopolitical context (EU) that is often under-researched. This study could help policy regulators, lawyers, civil society organizations, ISPs, and other entities to understand whether and how blocking websites and network services occur in a given country or region.

ACKNOWLEDGMENTS

The authors would like to thank the nobloc entity and the sincensura [48] group for their very valuable contribution during the collection and the analysis of network measure ments for their very valuable help during the analysis of network measurements. Furthermore, the authors also acknowledge all the anonymous reviewers for their valuable comments.

Additionally, the authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No 639379-DATACTIVE, awarded to Stefania Milan as Principal Investigator) [17].

REFERENCES

[1] Giuseppe Aceto, Alessio Botta, Antonio Pescapè, M. Faheem Awan, Tahir Ahmad, and Saad Qaisar. 2016. Analyzing Internet Censorship in Pakistan. In *Research and Technologies for Society and Industry*. IEEE.

[2] Giuseppe Aceto and Antonio Pescapè. 2015. Internet Censorship detection: A survey. *Computer Networks* 83 (2015), 381–421.

[3] ACN. 2019. Spain passes decree to shut down websites and social media over public order threats. https://www.catalannews.com/politics/item/spain-passes-decree-to-shut-down-websites-and-social-media-over-public-order-threats

[4] Walid Al-Saqaf. 2016. Internet Censorship Circumvention Tools: Escaping the Control of the Syrian Regime. *Media and Communication* 4, 1 (2016).

[5] Collin Anderson. 2013. *Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran.* Technical Report. University of Pennsylvania.

[6] Andy. 2015. Block Pirate Bay in 72 Hours. https://torrentfreak.com/block-pirate-bay-in-72-hours-spanish-court-tells-isps-150327/

[7] Christina Angelopoulos. 2009. Filtering the Internet for Copyrighted Content in Europe. *IRIS plus 2009-4, European Audiovisual Observatory* (2009).

[8] Web Archive. 2019. eln-voces.com - This Domain Has Expired. https://web.archive.org/web/20190716230422/http://www.eln-voces.com/

[9] Simurgh Aryan, Homa Aryan, and J. Alex Halderman. 2013. Internet Censorship in Iran: A First Look. In *FOCI*. USENIX.

[10] RIPE Atlas. 2020. RIPE. https://atlas.ripe.net

[11] Alex Barrera. 2014. ¿Que? A judge has ordered the blockage of Uber's website in Spain. https://tech.eu/news/court-shutdown-uber-spain/

[12] Simone Basso. 2020. Evaluating OONI's New Measurement Engine. (May 2020). https://ooni.org/post/2020-engine-evaluation-spain/

[13] Simone Basso. 2021. Aladdin: Experimental Web Connectivity implementation. https://github.com/bassosimone/aladdin

[14] Andreas Busch, Patrick Theiner, and Yana Breindl. 2017. Internet Censorship in Liberal Democracies: Learning from Autocracies? In *Managing Democracy in the Digital Age*. Springer International Publishing, 11–28.

[15] Abdelberi Chaabane, Terence Chen, Mathieu Cunche, Emiliano De Cristofaro, Arik Friedman, and Mohamed Ali Kaafar. 2014. Censorship in the Wild: Analyzing Internet Filtering in Syria. In *Internet Measurement Conference*. ACM.

[16] Council decision (CFSP) 2017/1426 2017. https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX%3A32017D1426&from=EN

[17] DATACTIVE. 2021. The Politics of Data According to Civil Society. https://data-activism.net

[18] Comisión Nacional de los Mercados y la Competencia. 2020. CNMCData - Informe Trimestral.

[19] Roya Ensafi, Philipp Winter, Abdullah Mueen, and Jedidiah R. Crandall. 2015. Analyzing the Great Firewall of China Over Space and Time. *Privacy Enhancing Technologies* 2015, 1 (2015).

[20] Fortinet. 2019. Deep inspection. https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/122078/deep-inspection.

[21] Fortinet. 2020. FortiOS Security Profiles. https://help.fortinet.com/fos50hlp/52data/Content/FortiOS/fortigate-whats-new-52/securityprofiles.htm.

[22] Qurium Media Foundation. 2020. Blocking Techniques Catalunya. https://www.qurium.org/alerts/spain/blocking-techniques-catalunya.

[23] Genevieve Gebhart, Anonymous Author, and Tadayoshi Kohno. 2017. Internet Censorship in Thailand: User Practices and Potential Threats. In *European Symposium on Security & Privacy*. IEEE.

[24] Devashish Gosain, Anshika Agarwal, Sahil Shekhawat, H. B. Acharya, and Sambuddho Chakravarty. 2017. Mending Wall: On the Implementation of Censorship in India. In *SecureComm*. Springer.

[25] Arne Hintz and Stefania Milan. 2018. "Through a Glass, Darkly": Everyday Acts of Authoritarianism in the Liberal West. *International Journal of Communication* 12 (2018), 3939–3959.

[26] Ralph Holz, Jens Hiller, Johanna Amann, Abbas Razaghpanah, Thomas Jost, Narseo Vallina-Rodriguez, and Oliver Hohlfeld. 2020. Tracking the Deployment of TLS 1.3 on the Web: A Story of Experimentation and Centralization. *SIGCOMM Comput. Commun. Rev.* 50, 3 (July 2020), 315.

[27] OpenNet Initiative. 2020. Internet Filtering in Burma in 2005: A Country Study. https://opennet.net/studies/burma.

[28] Gunnar Eyal Wolf Iszaevich. 2019. Distributed Detection of Tor Directory Authorities Censorship in Mexico. IARIA.

[29] Tord Lundström and Maria Xynou. 2017. Evidence of Internet censorship during Catalonia's independence referendum. https://ooni.torproject.org/post/internet-censorship-catalonia-independence-referendum/

[30] Gurmeet Singh Manku, Arvind Jain, and Anish Das Sarma. 2007. Detecting near-duplicates for web crawling. In *Proceedings of the 16th international conference on World Wide Web - WWW '07*. ACM Press.

[31] Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert, and Vern Paxson. 2015. An Analysis of China's "Great Cannon". In *Free and Open Communications on the Internet*. USENIX.

[32] Matthias Brugger. 2017. *Internet censorship in the Catalan referendum.* https://mirror.netcologne.de/CCC/congress/2017/slides-pdf/34c3-9028-internet$_c$ensorship$_i$n$_t$he$_c$atalan$_r$eferendum.pdf

[33] Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed, and Neha Kumar. 2017. When the Internet Goes Down in Bangladesh. In *Computer-Supported Cooperative Work and Social Computing*. ACM.

[34] Zubair Nabi. 2013. The Anatomy of Web Censorship in Pakistan. In *Free and Open Communications on the Internet*. USENIX.

[35] Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill. 2020. ICLab: A Global, Longitudinal Internet Censorship Measurement Platform. In *Proceedings of the*

41st IEEE Symposium on Security and Privacy.
[36] Women on Web. 2021. Courtcase against Spanish government for blocking abortion website during COVID19 @ Women on Web. (2021). https://www.womenonweb.org/en/page/20678/courtcase-against-spanish-government-for-blocking-abortion-website
[37] OONI. 2019. Web Connectivity test specification. https://github.com/ooni/spec/blob/ba7e41442ca13226d2594f46845938f1c33de38c/nettests/ts-017-web-connectivity.md.
[38] OONI. 2020. OONI: Open Observatory of Network Interference. https://ooni.org
[39] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. 2017. Global Measurement of DNS Manipulation. In *USENIX Security Symposium*. USENIX.
[40] Marta Poblet. 2018. Distributed, privacy-enhancing technologies in the 2017 Catalan referendum on independence: New tactics and models of participatory democracy. *First Monday* 23, 12 (2018).
[41] J. Postel and J. Reynolds. 1994. *Assigned Numbers*. RFC 1700. RFC Editor. https://www.rfc-editor.org/rfc/rfc1700.txt
[42] Ram Sundara Raman, Prerana Shenoy, Katharina Kohls, and Roya Ensafi. 2020. Censored Planet: An Internet-wide, Longitudinal Censorship Observatory. In *Computer and Communications Security*. ACM.
[43] Ram Sundara Raman, Adrian Stoll, Jakub Dalek, Reethika Ramesh, Will Scott, and Roya Ensafi. 2020. Measuring the Deployment of Network Censorship Filters at Global Scale. In *Network and Distributed System Security*. The Internet Society.
[44] Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. 2020. Decentralized Control: A Case Study of Russia. In *Network and Distributed System Security*. The Internet Society.
[45] Pekka Savola. 2018. Internet Connectivity Providers as Involuntary Copyright Enforcers: Blocking Websites in Particular. (March 2018), 300.
[46] Maria José Schmidt-Kessen, Julia Hörnle, and Alan Littler. 2019. Preventing Risks from Illegal Online Gambling Using Effective Legal Design on Landing Pages. *SSRN Electronic Journal* (2019).
[47] SecurityTrails. 2020. Domain Security, DNS Trails and IP Tools. https://securitytrails.com/
[48] Sincensura. 2021. https://sindominio.net/sincensura/en
[49] Paul Sturges. 2008. Access Denied: The Practice and Policy of Global Internet Filtering. *The Electronic Library* 26, 6 (Nov. 2008), 924–925.
[50] Rima Tanash, Zhouhan Chen, Dan Wallach, and Melissa Marschall. 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.
[51] Rima S. Tanash, Zhouhan Chen, Tanmay Thakur, Dan S. Wallach, and Devika Subramanian. 2015. Known Unknowns: An Analysis of Twitter Censorship in Turkey. In *Workshop on Privacy in the Electronic Society*. ACM.
[52] Benjamin VanderSloot, Allison McDonald, Will Scott, J. Alex Halderman, and Roya Ensafi. 2018. Quack: Scalable Remote Measurement of Application-Layer Censorship. In *USENIX Security Symposium*. USENIX.
[53] Ververis Vasilis. 2021. Network measurements analysis of Spanish ISPs. (2021). https://doi.org/10.5281/zenodo.4743905
[54] Vasilis Ververis, Fadelkon, Ana, Bita, and Samba. 2020. Women on Web website censored in Spain. https://blog.magma.lavafeld.org/post/women-on-web-blocking/ Magma.
[55] Vasilis Ververis, Marios Isaakidis, Chrystalleni Loizidou, and Benjamin Fabian. 2017. Internet Censorship Capabilities in Cyprus: An Investigation of Online Gambling Blocklisting. In *E-Democracy*. Springer.
[56] Vasilis Ververis, George Kargiotakis, Arturo Filastò, Benjamin Fabian, and Afentoulis Alexandros. 2015. Understanding Internet Censorship Policy: The Case of Greece. In *Free and Open Communications on the Internet*. USENIX.
[57] Tarun Kumar Yadav, Akshat Sinha, Devashish Gosain, Piyush Kumar Sharma, and Sambuddho Chakravarty. 2018. Where The Light Gets In: Analyzing Web Censorship Mechanisms in India. In *Internet Measurement Conference*. ACM.

A BLOCKPAGE

This section provides the switch statement blockpage analyzed in Section 3.1.2. The complete data with all the blockpages are available in [53].

```
<!DOCTYPE html PUBLIC \"-//W3C//DTD␣HTML␣4.01//EN\">
<!--
CATEGORY:  Judicial_Guardia_Civil
DEST_IP:  107.180.40.196
FGT_HOSTNAME:  RFFBTB1-02
SOURCE_IP:  [REDACTED]
-->
<html>
  <head>
    <meta charset="utf-8"/>
    <title id="4">
      Judicial_Guardia_Civil
    </title>
  </head>
  <body>
    <CENTER>
      <h1 id="causa" name="Judicial_Guardia_Civil">
      </h1>
      <script type="text/javascript">
        var name = document.getElementById("causa").getAttribute('
            ↪name');
        var text = "";
        var f = new Date();
        var mes=f.getMonth()+1;
        var dia=f.getDate();
        var hora=f.getHours();
        var minu=f.getMinutes();

        if (mes<10) mes="0"+mes;
        if (dia<10) dia="0"+dia;
        if (hora<10) hora="0"+hora;
        if (minu<10) minu="0"+minu;

        switch (name) {
          case "PHISHING_TSOL_MENSAJE_1":
            text = "PTM1_Judicial_Policia_Nacional";
            window.location.replace("http://a.policia.es/?url=www.
                ↪eln-voces.com/");
            break;
          case "Administrativo_Ley_del_Juego":
            text = "Administrativo_Ley_del_Juego";
            window.location.replace("http://192.187.20.203");
            break;
          case "Judicial_Guardia_Civil":
            text = "Judicial_Guardia_Civil";
            window.location.replace("http://82.223.97.47");
            break;
          case "Judicial_Policia_Nacional":
            text = "Judicial_Policia_Nacional";
            window.location.replace("http://
                ↪webbloqueadaporpolicianacional.com");
            break;
          case "Direccion_General_de_la_Policia":
            text = "Direccion_General_de_la_Policia";
            window.location.replace("http://a.policia.es/?url=www.
                ↪eln-voces.com/");
            break;
          default:
            text = "ERROR␣404␣-␣'Judicial_Guardia_Civil'␣not␣found
                ↪";
        }
        document.getElementById("causa").innerHTML = text;
      </script>
    </CENTER>
  </body>
</html>
```

Listing 1: AS3352 Blockpage of byte size 2374 (Fortigate)