Understanding Internet Censorship Policy: The Case of Greece

Vasilis Ververis
Humboldt University Berlin

George Kargiotakis

Arturo Filastò
The Tor Project

Benjamin Fabian
Humboldt University Berlin

Afentoulis Alexandros

Abstract

The Greek government has recently initiated large scale content blocking that leads to Internet censorship. In this article we analyze the techniques and policies used to block content of gambling websites in Greece and present the implications of the detected underblocking and overblocking. We have collected results probing eight major broadband and cellular Internet Service Providers (ISPs) that are a representative sample of Internet usage in Greece, and investigate the methods and infrastructure used to conduct the content filtering. The results of this study highlight issues related to how transparently Internet filtering is implemented in democratic countries and could indicate the presence of unfair competition between ISPs.

1 Introduction

There are many incidents of Internet censorship, which have usually been reported from countries without democratic political systems. In the following article we present methods and techniques to investigate Internet censorship based on empirical measurements. Furthermore, we present a case study from a democratic country where we analyze the state of censorship in depth, demonstrating the viability and usefulness of our approach.

In Greece, there have been several incidents reported that indicate ongoing issues of Internet censorship. Starting as early as October 2006, the administrator of a Greek blog RSS aggregator service blogme.gr has been sued, arrested and jailed for hosting a link via an RSS (Rich Site Summary) feed from a blog post containing allegedly offending content [11]. As a consequence, the server of blogme.gr was shut down, the hard drives and the computer systems used by the server administrator were confiscated even though the service provided by blogme.gr was unrelated in any way other than linking the offending blog post via automatic RSS syndication.

In February 2010 ISP Tellas/Wind Hellas blocked the Piratebay site [1]. In May 2012 the Greek Organization for Intellectual Property Collective Administration (AEPI) went to court against every Greek ISP demanding to censor Ellinadiko.com, a music sharing forum and Music-Bazaar.com, an MP3 webstore, both under the accusation of infringing copyright laws [2]. The court ordered the ISPs to block the IP addresses of the referred websites [23].

Later in September 2012 a citizen was arrested on charges of malicious blasphemy and religious insult after posting a Facebook page that ridiculed a well-known Greek Orthodox monk [12]. Following in January 2013, a politician filed a defamation lawsuit against a Greek Wikipedia user and administrator, insisting to remove content hosted on a Greek Wikipedia page related to his name. Nonetheless he sued the Greek Free / Open Source Software society that he mistakenly believed to be the organization running the Wikipedia project [13].

In this article we will focus on censorship implied by content regulation policies, and particularly an anti-gambling policy in article 52, law No. 4002/2011 [5]. So far, there have been only very few and selective data reports available to conduct research in this field in terms of studies regarding the type of censorship taking place and the techniques used in order to observe the criteria set by censors. Our article will try to close this research gap by systematic empirical measurements across multiple ISPs. The selected set of ISPs account for the majority of the fixed and wireless broadband customers [40], [41].

The rest of the article is structured as follows. First we present related work in Section 2. Then, in Section 3, we present our methodology, the infrastructure and tools used to conduct our censorship research. Following we provide an analysis of the collected set of data per blocking method and ISP in Section 4. Continuing in Section 5 we analyze the blacklist used to conduct the blocking of the resources, we reveal how the ISPs ”broke” the

email communication with these websites. Conclusions are given in Section 6.

2 Related Work

So far to the authors' best knowledge there is minimal technical literature based on Internet censorship in the western world. Breindl et al [43] examine the debates surrounding network filtering in France and Germany, focusing on the arguments used by opponents and proponents of Internet blocking. The authors analyse the outcomes and, the various challenges posed by Internet blocking to democracy. Aase et al [44] collected measurements and social sciences aspects from three different contexts; public wireless networks in USA and microblogging and chat programs in China. By this comparison they attempt to illustrate the importance of the elements of motivation, resources and time in Internet censorship.

Furthermore we are providing a brief description of some censorship related research located outside the western world which we consider relevant as it provides a technical perspective related to our research focus. Wright et al [45] examine the problem of Internet censorship from a user perspective rather than on a national level. In their paper they discuss the possibility to detect the effects of Internet filtering thought different providers and services. In a recent article [25] Geddes et al. presented the arising issues when using covert communication channels to circumvent Internet censorship. In his revision of an anti-censorship technologies taxonomy, Leberknight et al. discusses the challenges and opportunities of censorship resistant systems [26]. An in-depth analysis by Nabi [27] provides a time-line (starting from 2006) on the implemented censorship activities in Pakistan. He analyses a variety of technical methods being used and provides some trivial censorship circumvention options. In the same context Arya et al [28] examined Iranian censoring techniques and tools applied. Their work consists of a topographical map that enumerates the categories of the censored websites. Further contributions regarding Internet censorship include reports that have been gathered by the OONI project on several countries, including Zambia [29], Palestina [30], USA [32], Uzbekistan and Turkmenistan [31].

3 Methodology

In our censorship research we have used a variety of common Free and Open Source Software networking tools for gathering, categorizing, distributing, analyzing data and comparing the results. Since acquiring results from many ISPs is crucial to form a representative sample, we have probed five ISPs offering landline broadband connections and three cellular mobile operators during our research. An analysis can be found in Section 4

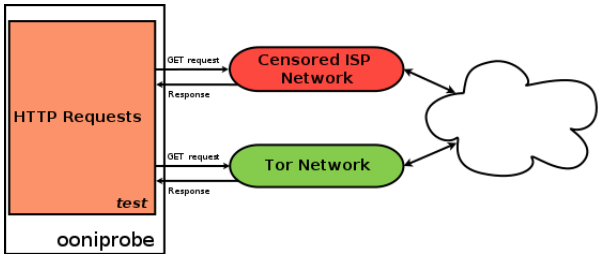

Figure 1: Ooniprobe HTTP request test diagram

3.1 Set of Data Used for the Tests

We have used the blacklists issued by the Hellenic Gaming Commission (EEEP) (see Section: 5.2), titled:*"List of sites providing gaming and betting services without authorization in Greece"*. The newly formed Independent Administrative Authority's Hellenic Gaming Commission acts as the public body responsible for the control and supervision of gambling services in Greece and publishes a blacklist of websites that are offering unlicensed gambling and betting services to Greek Internet users. According to article 52, law No. 4002/2011, A180 [5] gambling and betting websites without a license specifically for the Greek market is a serious criminal offense for users (players) that interact with or via these websites, but also for companies that run gambling businesses and ISPs that allow users to access the unlicensed websites.

The blacklist was transmitted to 211 ISPs, credit institutions and competent prosecuting authorities (misdemeanors Athens prosecutor, financial and e-crime prosecution department of financial police). According to [22] each entry in the blacklist has been revised by EEEP and was checked by two different echelons, through checks carried out on two different days and at different times-of-day [22].

3.2 Collection of Censorship Analysis Reports

The collection of the network measurements took place during the months of June and August 2014. For our censorship research we used ooniprobe [21], an application developed by the OONI project [14] used by users and organizations to probe their network for signs of network tampering, surveillance or censorship. Developed with the idea of ensuring the detection of any interference

```
Certain censorship: 300
Certain censorship (single requests): 57
Possible censor mistakes (404): 72
Total Censored (Certain + Single +
    ↪ Mistakes): 429
----
Total Single responses: 65
Single responses over Tor (exclude from
    ↪ stats): 0
Control failure: 18
```

Listing 1: Reports Parser Output

```
dig +short A www.netbet.com @213
    ↪ .249.17.10
Response: 213.249.29.111

dig +short A netbet.com @213.249.17.10
Response: (no answer)

dig +short A sport.netbet.com @213
    ↪ .249.17.10
Response: (no answer)
```

Listing 2: DNS responses of 'netbet.com' entries

with network communications, it aims to collect and provide high quality reports by using open and transparent data methodologies freely available to anyone that would like to process, read and research using a standard common file format (YAML).

Ooniprobe is the application being used to conduct the measurements on the ISP networks (both landline and cellular networks) where we detected network tampering and content blocking (see Section 4). Ooniprobe provides a variety of test cases and classes that could be used to probe the networks. In our research we have deployed the HTTP Requests test [15]. This performs an HTTP GET request from a specified list of URLs containing potentially censored websites over the test network (censored ISP network) and over the Tor network; the process is illustrated in Figure 1. It then compares the response headers and checks if the two responses (the one over Tor and the one over the censored network) match and if the proportion of differences between the expected body lengths is under a specific threshold. In our test cases we have used a tolerance factor of 80 percent between the two body lengths. The page body length difference was proven to be the most effective similarity indicator [42]. Moreover, in order to avoid false positives, results were further analysed by hand. See Appendix A.2 for a summary of an ooniprobe test.

For the collection and storage of ooniprobe reports we have used remotely manage Raspberry Pi embedded devices. The small footprint, minimal cost and power requirements make Raspberry Pi an ideal candidate for distributing it across individuals and organizations, who would like to contribute results by probing their network for instances of censorship. We have implemented Lepidopter; a custom boot image [34] based on Debian GNU/Linux offering a ready to boot image that eases the installation, configuration, as well as management and assist in the execution of ooniprobe network measurements tests. Apart from our network measurements Lepidopter aims to increase the coverage of censored networks around the world. The distribution image with the source code is freely available under the GNU general public license version 3 [34]. Our network measurements have been collected from multiple probes and locations under the same ISPs. Specifically, we have used at least two different probes per ISP and conduct measurements on different days and time frames to provide consistent reports. Initially, we have encountered inconsistent results between same ISPs on different connections. The cause of these inconsistencies were due to the DNS resolvers being used, since many of the ISPs use DNS Hijacking to enforce the blocking implied by EEEP. Additionally, we have identified that some of the ISPs were blocking the TCP requests to port 443, which resulted to a network timeout when a probe (or a user) was trying to access any URL entries from the EEEP blacklist. Note that the users should be receiving a block page (see Figure 2) that provides information on why this URL (or domain name) is blocked rather than a network timeout that could confuse the users to think that there is some network or server failure.

The size of each result set, over 10 MiB, makes it very impractical to easily extract results. To be able to extract meaningful information from ooniprobe's YAML output we have created a sample parser in python. The parser looks for a number of criteria in the headers or body of the test results from ooniprobe and if there's a match, it categorizes the test as being censored or not. Among these criteria there is a check for *headers_match* parameter of ooniprobe tests, a check for ISP redirect URLs in response headers and a search for *gamingcommission.gov.gr* in response body. The parser also catches some ooniprobe test failures, for example not being able to fetch results over Tor. Finally, it displays a summary of the parser output (see Listing 1).

In this section we are reviewing and processing the results taken from eight major Greek ISPs, five of them offering standard landline services (Cyta, Hol, Forthnet, Ote, Wind) while the other three ISPs are offering mobile services (Cosmote, Vodafone, Wind).

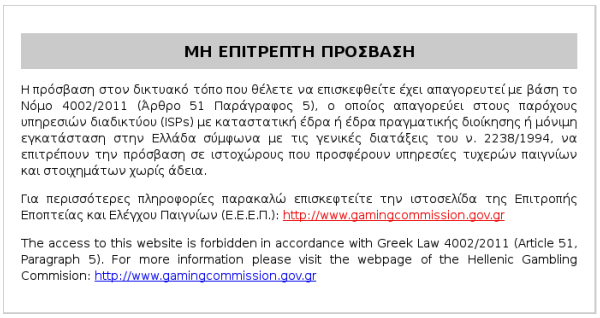

Figure 2: Blocked Webpage Screenshot

4 Analysis of Blocking per ISP

Most Greek ISPs have not issued any public report that notifies their customers and users about the content blocking of the EEEP blacklist. On 2 August 2014, we contacted all ISPs via email communication, mentioning our research and the related network measurements. We have inquired the ISPs for clarification about their filtering policies, specifically how they renew the blacklist, and by which technical means and implementations the blocking of the content takes places. Additionally, we have asked them to inform us how they communicate the content blocking with their customers. Finally, we have sent a request for comments regarding the blocking regulation imposed by EEEP, how the process could be improved and if they are forced to block other content upon request or based on another blacklist. Out of the eight ISPs representatives and support teams that we contacted, only one (Cyta) replied and directed us to the EEEP website [17] which was irrelevant to our specific inquiries. In our reply we repeatedly pointed to our inquiries but as of the date of this article submission no further email communication was received.

4.1 Blocking Methods

4.1.1 DNS Hijacking

ISPs are in control of the DNS servers being used by their clients' xDSL routers. Since they can manipulate their DNS servers' responses, they can redirect the requesting clients to anywhere they want. Taking advantage of this privilege, ISPs modify their resolvers to override censored domains' legitimate DNS replies by creating local zone entries [35]. These entries usually point to a server that they control where they run a web server that displays a censorship warning message to the users.

4.1.2 Deep Packet Inspection

Deep Packet Inspection (DPI) is the basis of the most advanced form of censorship. Special appliances have the ability not only to look into Layer 3 and Layer 4 headers but to also look inside the payload of each and every packet. They can distinguish packets going to a server and either stop them from reaching their target, change the server's response, or even redirect the packets to another server. These devices perform a hostile, active, man-in-the-middle attack on every client connecting to the network, Internet or Intranet, through them.

In the following, we enumerate the amount of blocked entries and the blocking methods used by the ISPs to censor access to web resources. Figure 2 illustrates the landing blocked webpage.

4.2 ISP Analysis

Cosmote ISP (AS 29247) has blocked all the entries of the published blacklist. The HTTP headers included in the hijacked response indicate the presence of an Apache/2.2.15 web server running on a Linux based OS (CentOS). The implied method of blocking is DNS hijacking and the indication of censorship includes the URL string *http://www.gamingcommission.gov.gr/index.php/el/* in the body of the HTTP response.

Cyta ISP (AS 6866) has blocked 81.5% entries of the published blacklist. The collected HTTP headers indicate the use of the Apache web server. The method of blocking used is DNS hijacking and 404 HTTP errors. During our network measurements, we detected at least 80 blacklist entries incorrectly responded with a 404 HTTP error, *"Not Found"* instead of displaying the filtering warning page. Even though this is probably because of a misconfiguration of the ISPs' web server hosting the warning page, this technique (the fake 404 HTTP error) results in the user not knowing the reason why the resource is inaccessible and is therefore a transparency issue. Such censorship technique has reportedly been used in many countries already [3], [4]. The HTTP response body contains the URL string *http://www.gamingcommission.gov.gr/index.php/el/* but only for the entries that return a blocking page. We have been able to identify the fake 404 HTTP errors by comparing the results with other ISPs. Cyta introduces a Google Analytics script on their blocking webpage [16] which can be used to track users that have tried to access the blocked content. Although the blocking page is hosted on the same website (Cyta main website) the user tracking application differs.

Forthnet ISP (AS 1241) has blocked 21.91% of the published blacklist. This is the lowest percentage of

ISP	Blocked Entries	Blocking Method	Server Fingerprint	Overblocking
Cosmote	438 (100%)	DNS Hijacking	Apache/2.2.15 (CentOS)	✗
Cyta	357 (81.5%)	DNS Hijacking, HTTP 404	Apache	✓
Forthnet	96 (21.91%)	DNS Hijacking	BigIP	✓
Hol	438 (100%)	DNS Hijacking	lighttpd/1.4.31	✓
Ote	438 (100%)	DNS Hijacking	Apache/2.2.15	✓
Wind	325 (74.2%)	DNS Hijacking, HTTP 404	Tellas HTTP Server	✗
Wind Mobile	325 (74.2%)	DNS Hijacking, HTTP 404	Tellas HTTP Server	✗
Vodafone	425 (97.03%)	DNS Hijacking, DPI	WebProxy/6.0	✗

Table 1: Per ISP list of server fingerprints, overblocking indication, blocked entries and methods

blocked URLs among all ISPs, and this fact is quite known to the Greek gambling community who advise users that experience blocking to switch to this ISP. The number of subscribers of this ISP has been steadily increasing since 2013 [18], bursting the total subscriptions to a historical record of 1,145,948 [19]. The server fingerprint collected by the HTTP headers indicate the use of Big IP as part of the network filtering infrastructure. Upon receiving the hijacked DNS response the user is being redirected (HTTP 302) to the blocked page URL *http://eeep.forthnetgroup.gr*.

HOL ISP (AS 3329) has blocked all entries of the published blacklist. The HTTP headers collected state the use of a lighttpd web server software (with build version 1.4.31). This ISP returns a fake DNS response that redirects (HTTP 301 code) the user to the blocking page with URL string *http://eeepnotice.hol.gr/*.

OTE ISP (AS 6799) has blocked all the entries of the published blacklist. It is the only ISP that takes care to preserve the DNS mail (MX) records for some of the filtered domains. The HTTP headers (Apache/2.2.15 (CentOS)) and the URL string returned on the response HTTP body (http://www.gamingcommission.gov.gr/index.php/el/) extracted from our measurements are identical with the Cosmote ISP, which is part of the same company group.

Wind (AS 25472) and **Wind mobile** (AS 15617) ISPs (same company group) have blocked 74.2% of the published blacklist. The HTTP headers include the string *Tellas HTTP Server*. Apart from the DNS hijacking blocking method, we detected that at least 65 entries erroneously responded with a 404 HTTP error. Four other entries of the blacklist were redirecting to a page of the Wind ISP website with the HTTP body string *"landline services provided by Wind have been suspended"*. These ISPs mislead users by not providing them with the block page that informs about the gambling law.

Vodafone ISP (AS 12361) uses DNS hijacking for 58 entries that EEEP has published either using HTTPS URLs on the blacklist or entries that are not prefixed with *http://* (the blacklist entries can be found in [39]. For the rest of them it uses some kind of DPI/proxy, using Bluecoat's WebProxy/6.0. If an HTTP URL does not exactly match the one published at the blacklist it is passed on to the original server, if it matches then the request gets redirected to *http://1.2.3.50/ups/no_access_gambling.htm*. The process of determining the DPI blocking by Vodafone is presented in Appendix A.1.

Another interesting case with this ISP is that for domains that it has filtered using DNS hijacking, subdomains of those do not even have an A record (dns_lookup_error). That means that some URLs on the blacklist that contain subdomains are not getting redirected to *http://1.2.3.50/ups/no_access_gambling.htm*, they cannot be resolved and are not accessible at all from clients. We use the DNS lookup utility dig and queried the A DNS records for the resources *www.netbet.com*, *netbet.com* and *sport.netbet.com* using Vodafone NS. Out of the three queries only one (*www.netbet.com*) provided a response which pointed to the host of Vodafone used for blocking. The DNS lookup queries are listed in Listing 2. Vodafone ISP has blocked 425 entries of the published EEEP blacklist, 15 of them returned DNS lookup errors.

4.3 Collateral Damage

In an announcement [20] published by the commission addressing the public about the blacklist, they reply to the question: *"How will (gambling) players be able to contact the companies since they are now blocked?"* and their response is: *"By advising people to look at their previous bank transactions where contact details of these companies might exist"*. If the ISPs were actually blocking URLs, then emails towards the companies would still work, but because ISPs interfere and manipulate the DNS records of the blocked sites, most of them do not even pay attention to the DNS Mail eXchanger (MX) records of the gambling companies domains, and a user cannot email them any more since an MX record points to the appropriate mail server and specifies how email delivery

should be routed for a given domain name.

In the process to deliver an email, an SMTP client will first query the destination domain for an MX record and if no record is found, it will fall back to look up an A record (or AAAA record if IPv6 is available) for the domain in question and attempt to deliver email based on these records. Apparently, without any MX records or legitimate A records for the blacklisted domains in question email delivery would be impossible. During our research, we found out that most ISPs have hijacked the MX records of the domains included in the EEEP blacklist.

In our case the ISPs have spoofed the A records of the gambling domains to point to a local server or a proxy server. As a result, any email delivery will fail and the user will only realize this after hours or even days (depending on their SMTP server configuration). This implies tremendous negative impacts and leads to a restriction of fair markets and business regulations, i.e., a user trying to communicate with any business (all of the censored websites are businesses) will find himself unable to do so. Out of eight ISPs only one (Ote ISP) found to sync the MX records from some (but not all) of the blacklisted domains. However, it remains unclear if and how often these records are updated.

5 Blacklist Analysis

5.1 Blacklist Distribution

The method that EEEP uses to distribute the blacklist to the ISPs remains unclear. Sources from ISPs claim that they have never received any updates apart from the very first time that the blacklist was communicated to them. At that time they were given instructions to visit the EEEP website [33] and manually download the blacklist. Since then, there have been three updates to the original blacklist released, all of them only published on EEEP's website in the form of PDF files. One would have expected that the blacklist was at least in a machine parsable format to automate the procedure, but that is not currently the case. So far, there is no automated way to check for updates of the blacklist, the downloadable PDF changes filename each time there's an update, and there is no Application Programming Interface (API) to query for updates. The published PDF is not signed by any authority but at least EEEP's website is using HTTPS and is redirecting all HTTP requests to their HTTPS equivalent URLs.

5.2 EEEP Blacklist Analysis

Starting in July 2013 [22], EEEP published a blacklist [6] containing 401 entries of URLs that do not comply with the regulations of EEEP as analyzed in Section 3.1. Later in November 2013, there were 22 new entries added to the blacklist [7]. Following that, in February of 2014 there were 25 further entries added [8]. Finally, in July 2014 [9] there was one entry removed, summing up the blacklisted entries to 437. Our measurements tests took place between June and July 2014, using the third released version of the blacklist [8].

Upon the latest blacklist update [9] the entry: *http://www.pokerstarsblog.com/* was removed from the blacklist. We have probed again all ISPs to check if they have complied with the update of the EEEP blacklist, unfortunately many of them were still blocking the entry, the results (overblocking column) are listed in Table 4. The complete blacklisted entries can be found in [39].

Throughout the blacklist analysis we determined that the entries contain duplicate, malformed and unavailable entries. Malformed entries do not follow certain specifications such as URL canonicalization, contain spelling mistakes, and query parameters in URLs with reserved characters such as the strings `'#_'` and `'action='` that should be first encoded [10] prior to any distribution and publication of the blacklist.

- 28 entries (6.39%) are duplicate domains (with different URLs).
- 17 entries (3.88%) refer to pages or subdomains which are malformed.
- 3 entries (0.68%) are not hosting any gambling content (empty DNS A record, expired or parked domain names): *loosecannonholdem.com*, *unibet-1.com* and *venicegames.com*

While the Hellenic Gaming Commission has specifically asked for URL blocking, since it has posted a blacklist with URLs inside, ISPs would only be able to block them if they had previously installed some kind of DPI mechanism. That mechanism would give the ability to ISPs to look inside the payload of packets, and more specifically at the layer 7 contents where the actual URL of an HTTP request is referenced. A problem that arises though is what would have happened to the HTTPS URLs included in the blacklist. In order to be able to filter HTTPS URLs one needs to actually perform an active man-in-the-middle attack on every HTTPS connection in order to decrypt the SSL/TLS, layer it and look at the unencrypted payload.

Instead of filtering using DPI, all but one (Vodafone) of the aforementioned ISPs make use of DNS hijacking to block access to the blacklisted domains. This censorship method provides a different IP address of the requested domain/site than the actual one, redirecting the user to some other destination. Each ISP has chosen to

redirect users to a website of their own where they display a generic warning that the site is filtered.

We have discovered that the content blocking was sometimes implemented incorrectly and in many cases the users were not informed that a specific website adheres to the EEEP policy, leading them to assume that the website encountered a technical problem (HTTP 404 error or Connection timed out), which effectively obfuscates deliberate censorship. It is unclear how frequently the ISPs evaluate the effectiveness of their filtering rules, resulting in outdated and poorly implemented blacklists and in the surprising fact that none of them exactly complies with the EEEP policy. Unfortunately, without transparent methodologies and review on the blocking techniques it is quite difficult to be assured of the effectiveness of the filtering systems.

Furthermore, DNS hijacking can be quite easily circumvented and is highly ineffectual for blocking access to content, since the user could simply use a different DNS service. There are numerous issues introduced with DNS hijacking such as network security threats [35], phishing attacks [36] and privacy violation [37].

6 Conclusion

Throughout our research we highlighted flaws in the implementation of betting website censorship. Nevertheless, we do not aim for a properly implemented censorship of any kind. Instead, our intention is to make all those problematic issues visible, which arise when censorship is invoked as a method to approach a social or public issue.

ISPs in Greece have not provided any kind of notification to their customers informing them how the blocking took place, why this happened and if they can opt-out from the service. Lack of transparency on behalf of the providers permits them to block and censor arbitrary Internet destinations according to their needs, thus following a blocking-at-will strategy. Internet destinations may be accessible or not, while users have no reasoning about it. That would lead to deliberate abuse of citizens' accessibility and view of the Internet.

Censorship of some betting sites in Greece was implemented as a way to forbid residents of Greece to bet on websites that do not intend to pay taxes, whereas the claimed goal of the censors is to prevent players from betting. As examined in section 5, censorship implementations includes some major side-effects: users are not only forbidden to play on these websites, but they are also now unable to communicate (via email) with these companies. Censorship is thus not limited to a specific problem (tax evasion) but it is massively affecting user experience and communication.

7 Future Work

Based in our methodology described in Section 3.2 performing network measurements daily, weekly and upon renewal of the EEEP blacklist per ISP significantly improves the contribution of our research study. Furthermore, we consider our research study of gambling censorship a low risk, but high impact network measurement that could be applied to different countries ISPs.

References

[1] adslgr.com Technological Forum, Pirate Bay blocking, http://web.archive.org/web/20120112215459/http://www.adslgr.com/forum/showpost.php?p=3325943&postcount=14 , February 2010.

[2] Torrentfreak news portal, "Greek Court Orders ISP Blockades of Pirate Music Sites", http://web.archive.org/web/20140829222910/https://torrentfreak.com/greek-court-orders-isp-blockades-of-pirate-music-sites-120521 ,May 2012.

[3] Linx Public Affairs News, "BT Cleanfeed: the facts", http://web.archive.org/web/20140829222922/https://publicaffairs.linx.net/news/?p=154, September 2014.

[4] Noman Helmi, "Tunisian journalist sues government agency for blocking Facebook, claims damage for the use of 404 error message instead of 403", http://web.archive.org/web/20140829222940/http://opennet.net/node/950 ,Open Net Initiative, September 2008.

[5] Greek law, Law No. 4002/2011, Article 52, http://web.archive.org/web/20140829223000/http://nomoi.info/%CE%A6%CE%95%CE%9A-%CE%91-180-2011-%CF%83%CE%B5%CE%BB-44.html ,April 2012.

[6] EEEP Blacklist First Version, http://www.gamingcommission.gov.gr/images/apofaseis/lists/black%20list0001.pdf ,June 2013, Retrieved June 2014.

[7] EEEP Blacklist Second Version, http://www.gamingcommission.gov.gr/images/Anakoinoseis/BlackList_EEEP_%2022112013.pdf ,November 2013, Retrieved June 2014.

[8] EEEP Blacklist Third Version, http://www.gamingcommission.gov.gr/images/Anakoinoseis/BlackList_EEEP_%2021022014.pdf ,February 2014, Retrieved June 2014.

[9] EEEP Blacklist Fourth Version, https://www.gamingcommission.gov.gr/images/Anakoinoseis/BlackListVersion4_11072014.pdf ,July 2014, Retrieved July 2014.

[10] Tim Berners-Lee, Universal Resource Identifiers in WWW, http://web.archive.org/web/20140829223110/http://www.w3.org/Addressing/URL/uri-spec.html.

[11] Wikimedia Foundation Inc., "Greek blog aggregation service administrator jailed", http://web.archive.org/web/20140829223116/https://en.wikinews.org/wiki/Greek_blog_aggregation_service_administrator_jailed%2C_service_censored ,October 2006.

[12] Christos Syllas, Free speech takes a beating in Greece, Index on Censorship Organization, http://web.archive.org/web/20140829223121/http://www.indexoncensorship.org/2013/03/free-speech-takes-a-beating-in-greece/ , March 2013.

[13] Michelle Paulson, Wikimedia Foundation Inc., "Wikimedia Foundation supports Wikipedia user subject to defamation lawsuit in Greece", http://web.archive.org/web/20140829223131/https://blog.wikimedia.org/2014/02/14/wikimedia-foundation-supports-wikipedia-user-subject-to-defamation-lawsuit-in-greece/ , February 2014.

[14] Open Observatory of Network Interference Project http://web.archive.org/web/20140829223139/https://ooni.torproject.org .

[15] Ooniprobe Http Request Test Class http://web.archive.org/web/20140829223145/https://gitweb.torproject.org/ooni-probe.git/blob/HEAD:/ooni/nettests/blocking/http_requests.py .

[16] Block Landing Page, Cyta ISP http://web.archive.org/web/20140829223216/http://www.cyta.gr/misc/eeep_noaccess .

[17] EEEP, Press Release: "Responsible Play", http://web.archive.org/web/20140829223227/https://www.gamingcommission.gov.gr/index.php/el/ypefthino-paixnidi-ypmenu-im.

[18] Forthnet ISP, Press: Market Results 2013, http://web.archive.org/web/20140829223235/http://www.forthnet.gr/media/Company/anakinoseis/2014/FR%20Q4%202013%20press%20release_en.pdf ,March 2014.

[19] Euro2day News Portal, Forthnet Market Result First Quarter 2014, http://web.archive.org/web/20140829223245/http://www.euro2day.gr/news/enterprises/article/1219910/forthnet-afxhsh-esodon-lianikhs-kai-syndromhton-s.html ,May 2014.

[20] EEEP Blacklist Press Release, https://www.gamingcommission.gov.gr/images/apofaseis/lists/anakoinosi.pdf ,August 2013, Retrieved July 2014.

[21] Arturo Filasto, Jacob Appelbaum, In Proc. of: Free and Open Communications on the Internet, USENIX, 2012.

[22] EEEP Blacklist press release, July 2013, http://www.gamingcommission.gov.gr/images/deltia_tipou/dt2.pdf , Accessed July 2014.

[23] Court Ordered ISPs to Block IP Addresses, Greek Court Order, http://web.archive.org/web/20141114193131/https://www.void.gr/kargig/blog/wp-content/4658_2012.pdf ,May 2012.

[24] Ooniprobe Installation Instructions, https://github.com/thetorproject/ooni-probe#installation .

[25] John Geddes, Max Schuchard, and Nicholas Hopper, Cover your ACKs: pitfalls of covert channel censorship circumvention, In Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security (CCS '13). ACM, New York, NY, USA, 361-372.

[26] C. S. Leberknight, M. Chiang, H. V. Poor, and F. Wong. A taxonomy of Internet censorship and anti-censorship, 2010.

[27] The Anatomy of Web Censorship in Pakistan, Zubair Nabi In: Free and Open Communications on the Internet (Washington, DC, USA), USENIX.

[28] Internet Censorship in Iran: A First Look. Simurgh Aryan, Homa Aryan and J. Alex Halderman. In: Free and Open Communications on the Internet (Washington, DC, USA), USENIX.

[29] Zambia, a country under Deep Packet Inspection, OONI report, http://web.archive.org/web/20141005212653/https://ooni.torproject.org/zambia-a-country-under-deep-packet-inspection.html , July 2013.

[30] Hadara Palestine, OONI report, http://web.archive.org/web/20141115030108/https://ooni.torproject.org/hadara-palestine.html , April 2012.

[31] Tab-Tab, Come in! Bypassing Internet blocking to categorize DPI devices, OONI report, https://web.archive.org/web/20130926190044/https://ooni.torproject.org/tab-tab-come-in-bypassing-internet-blocking-to-categorize-dpi-devices.html , May 2013.

[32] T-Mobile USA Web Guard, OONI report, https://web.archive.org/web/20141115030554/https://ooni.torproject.org/t-mobile-usa-web-guard.html , March 2012.

[33] EEEP Official Website https://www.gamingcommission.gov.gr/

[34] Lepidopter, OONI powered Raspberry Pi image https://github.com/TheTorProject/lepidopter

[35] D. Atkins and R. Austein. Threat analysis of the domain name system (DNS). http://web.archive.org/web/20140826081656/http://www.ietf.org/rfc/rfc3833.txt , August 2004.

[36] D. Dagon, N. Provos, C. Lee, and W. Lee, Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority, in Proceedings of the Network And Distributed Security Symposium (NDSS), 2008.

[37] Florian Weimer. Passive dns replication. In 17th Annual FIRST Conference on Computer Security Incident Handling (FIRST 05), 2005.

[38] ICANN SSAC Report: Redirection in the Com and Net Domain http://web.archive.org/web/20141114231521/http://www.icann.org/en/system/files/files/report-redirection-com-net-09jul04-en.pdf , July 2004.

[39] OONI URL repository, EEEP Blacklist https://web.archive.org/web/20150514103452/https://github.com/hellais/ooni-inputs/blob/master/processed/bycountry/GR/urls/EEEP_Blacklist.txt , May 2015.

[40] Internet Service Providers - Greece, IPduh, http://ipduh.com/macro/gr/isp/ , Accessed May 2015.

[41] Internet service provider market share in Greece fourth quarter 2013, Point Topic, https://web.archive.org/web/20150514213631/http://point-topic.com/free-analysis/greece-broadband-overview/ , August 2014.

[42] Ben Jones and Tzu-Wen Lee and Nick Feamster and Phillipa Gill, http://conferences2.sigcomm.org/imc/2014/papers/p299.pdf , ACM Internet Measurement Conference 2014, Automated Detection and Fingerprinting of Censorship Block Pages

[43] Yana Breindl and Joss Wright, Internet Filtering in Liberal Democracies, Presented as part of the 2nd USENIX Workshop on Free and Open Communications on the Internet, 2012, Bellevue, WA, {https://www.usenix.org/conference/foci12/workshop-program/presentation/Breindl}, USENIX, Berkeley, CA

[44] Nicholas Aase and Jedidiah R. Crandall and Álvaro Díaz and Jeffrey Knockel and Jorge Oca Molinero and Jared Saia and Dan Wallach and Tao Zhu, Whiskey, Weed, and Wukan on the World Wide Web: On Measuring Censors' Resources and Motivations, https://www.usenix.org/system/files/conference/foci12/foci12-final17.pdf, USENIX, Free and Open Communications on the Internet, 2012

[45] Fine-Grained Censorship Mapping: Information Sources, Legality and Ethics, Joss Wright and Tulio Souza and Ian Brown, http://static.usenix.org/event/foci11/tech/final_files/Wright.pdf, USENIX, Free and Open Communications on the Internet, 2011

A Appendix

A.1 Vodafone DPI

In this section we demonstrate the case of DPI found in Vodafone ISP. We use the application curl to fetch the HTTP headers of the domain *rivernilecasino.net*, the request is not blocked and transmitted to the legitimate server of the domain. The response is listed in Listing 3.

```
HTTP/1.1 302 Moved Temporarily
Date: Sun, 31 Aug 2014 12:38:01 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Location: http://www.vegaspartnerlounge.
    ↪ com/generic/informer.asp?Subgid
    ↪ =987228&Country=Greece&btag=
    ↪ rivernilecasino.net&btag2=16&btag3
    ↪ =&btag4=&btag5=
Set-Cookie: RiverNileCasino=btag=
    ↪ rivernilecasino.net&btag2=16&btag3
    ↪ =&btag4=&btag5=; domain=
    ↪ rivernilecasino.net; expires=Mon,
    ↪ 01-Sep-2014 12:38:00 GMT; path=/;
    ↪ HttpOnly
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 279
Connection: keep-alive
```

Listing 3: HTTP headers of rivernilecasino.net

Similarly we change the URL to *www.rivernilecasino.net* (adding the *www* subdomain) and grab the HTTP headers, the request also passes through to the legitimate server. The response is listed in Listing 4.

```
HTTP/1.1 302 Moved Temporarily
Date: Sun, 31 Aug 2014 12:38:28 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Location: http://www.vegaspartnerlounge.
    ↪ com/generic/informer.asp?Subgid
    ↪ =785274&Country=Greece&btag=www.
    ↪ rivernilecasino.net&btag2=16&btag3
    ↪ =&btag4=&btag5=
Set-Cookie: RiverNileCasino=btag=www.
    ↪ rivernilecasino.net&btag2=16&btag3
    ↪ =&btag4=&btag5=; domain=
    ↪ rivernilecasino.net; expires=Mon,
    ↪ 01-Sep-2014 12:38:28 GMT; path=/;
    ↪ HttpOnly
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 283
Connection: keep-alive
```

Listing 4: HTTP headers of www.rivernilecasino.net

Finally using the same URL as the one published in the blacklist (*www.rivernilecasino.net/index.asp*), the request gets proxied via Vodafone ISP. The HTTP headers of the response is listed in Listing 5.

```
HTTP/1.1 301 Moved Permanently
Server: WebProxy/6.0
Date: Sun, 31 Aug 2014 12:39:01 GMT
Content-Length: 0
Location: http://1.2.3.50/ups/
    ↪ no_access_gambling.htm
Connection: keep-alive
```

Listing 5: HTTP headers of rivernilecasino.net

A.2 Reproducing the results with ooniprobe

We first install ooniprobe following the install instructions for our system [24]. We have used the command in Listing 6 to generate our reports the *file* parameter contains a formatted list of the EEEP blacklist [39]. The parameter "file" denotes the list of URLS to perform GET and POST requests. We have used a text file (EEEP_Blacklist.txt) with the blacklisted entries published from EEEP [39].

```
ooniprobe blocking/http_requests --file
    ↪ EEEP_Blacklist.txt
```

Listing 6: Running ooniprobe HTTP requests test

A.3 EEEP Blacklist Malformed Entries

http://backgammon.betoto.com/backgammon.aspx
http://betting.stanjames.com/Blog
http://casino.betoto.com/casino.aspx
http://casino.bwin.com/el/casino/home
http://el.pacificpoker.com/el/
http://en.betclic.com/
http://en.everestcasino.com/
http://en.expekt.com/
http://games.betoto.com/games.aspx
http://games.bwin.com/el/games/home
http://gr.sportingbet.com/stoixima-kazino-games-poker-bonus
http://home.betoto.com
http://i.spin3.com/rubyfortune/en
http://poker.betoto.com/poker.aspx
http://poker.bwin.com/el/poker
http://sports.bwin.com/el/sports
http://tatts.com/goldencasket
http://tatts.com/nswlotteries
http://tatts.com/tattersalls
http://tatts.com/tattsbet
http://t.rubyfortune.com/en/
http://web.boylesports.com/UK/1/BingoHome#action=bingohome
http://www.138sungame.com/en-gb
http://www.1bet.com/EN/index.html
http://www.1king.com/EN/casino.html
http://www3.bet90.com/en/
http://www.3dice.com/index.php
http://www.50starscasino.com/english/eur/index.html
http://www.777.com/play-blackjack.html
http://www.888sport.com/bet
http://www.allslotscasino.com/aq/aff/home.html#_
http://www.begado.eu/
http://www.betcasinograndbay.com/en/Index.html
http://www.betjupiterclub.com/Index.html
http://www.betlakepalace.com/Index.html
http://www.betroadhousereels.com/Index.html
http://www.betsson.com/start/el/
http://www.betvictor.com/sports/en
http://www.bulldog777.com/
http://www.bwin.com/default.aspx
http://www.casinoeuro.com/el/
http://www.casinokingdom.eu/
http://www.casinolasvegas.com/en/index.html
http://www.casinosplendido.com/
http://www.cherrygoldcasino.com/uk/
http://www.cosmikcasino.com/?lang=en
http://www.crowneurope.com/en/
http://www.deuceclub.com/?lang=en
http://www.domgame.com/
http://www.duel5.com/en-casino
http://www.everestcasino.com/en
http://www.firstwebcasino.com/#_
http://www.gowildcasino.com/en/
http://www.grandeaglecasino.com/en/index.html
http://www.grandonline.com/
http://www.harrycasino.com/en/
http://www.interwetten.com/el/Default.aspx
http://www.kerchingcasino.com/index.do
http://www.kingsolomons.com/greek/
http://www.lotusasiacasino.com/en-US/index.html
http://www.luckycreek.com/en/index.html
http://www.mandarinpalace.com/en-EU/index.html
http://www.maria.com/en
http://www.okonlinecasino.com/el/
http://www.palacevipcasino.com/english/usd/index.html
http://www.pkr.com/en/
http://www.planetcasino.com/uk/
http://www.portomasolive.com/portal/portal/index.jsp
http://www.redbet.com/en/
http://www.rivacasino.com/el/
http://www.rubyfortune.com/en/
http://www.scasino.com/en/index.html
http://www.slotastic.com/en/
http://www.slotsville.com/index.html
http://www.smartlivegaming.com/welcome.html
http://www.spinpalace.com/greek/
http://www.stanjames.com/Landing.aspx
http://www.sunbingo.co.uk/tv/movie/
http://www.suprocasino.com/en-gb/
http://www.vernons.com/home
http://www.wildjackcasino.com/#_
http://www.windowscasino.com/greek/
http://www.youwin.com/en