Measuring I2P Censorship at a Global Scale

Nguyen Phong Hoang
Stony Brook University

Sadie Doreen
The Invisible Internet Project

Michalis Polychronakis
Stony Brook University

Abstract

The prevalence of Internet censorship has prompted the creation of several measurement platforms for monitoring filtering activities. An important challenge faced by these platforms revolves around the trade-off between depth of measurement and breadth of coverage. In this paper, we present an opportunistic censorship measurement infrastructure built on top of a network of distributed VPN servers run by volunteers, which we used to measure the extent to which the I2P anonymity network is blocked around the world. This infrastructure provides us with not only numerous and geographically diverse vantage points, but also the ability to conduct in-depth measurements across all levels of the network stack. Using this infrastructure, we measured at a global scale the availability of four different I2P services: the official homepage, its mirror site, reseed servers, and active relays in the network. Within a period of one month, we conducted a total of 54K measurements from 1.7K network locations in 164 countries. With different techniques for detecting domain name blocking, network packet injection, and block pages, we discovered I2P censorship in five countries: China, Iran, Oman, Qatar, and Kuwait. Finally, we conclude by discussing potential approaches to circumvent censorship on I2P.

1 Introduction

Several platforms have been built to measure Internet censorship at a large scale, including the OpenNet Initiative [38], ICLab [58], Open Observatory of Network Interference (OONI) [32], Quack [75], Iris [64], and Satellite [68]. A common challenge faced by these platforms is the trade-off between depth of measurement and breadth of coverage.

In this paper, we present a complementary measurement infrastructure that can be used to address the above issue. The infrastructure is built on top of a network of distributed VPN servers operated by volunteers around the world. While providing access to many residential network locations, thus addressing the coverage challenge, these servers also offer the required flexibility for conducting fine-grained measurements on demand. We demonstrate these benefits by conducting an in-depth investigation of the extent to which the I2P (invisible Internet project) anonymity network is blocked across different countries.

Due to the prevalence of Internet censorship and online surveillance in recent years [7, 34, 62], many pro-privacy and censorship circumvention tools, such as proxy servers, virtual private networks (VPN), and anonymity networks have been developed. Among these tools, Tor [23] (based on onion routing [39,71]), and I2P [85] (based on garlic routing [24,25,33]), are widely used by privacy-conscious and censored users, as they provide a higher level of privacy and anonymity [42].

In response, censors often hinder access to these services to prevent their use [27, 29, 79]. Therefore, continuous measurements are essential to understand the extent of filtering and help in restoring connectivity to these networks for end users [19]. While many works have studied censorship on Tor [27, 29, 79] (OONI [32] even has a dedicated module to test connectivity to the Tor network), none have comprehensively looked into the blocking status of I2P. To fill this gap, in this work we investigate the accessibility of I2P using the proposed VPN-based measurement infrastructure.

Our analysis of 54K measurements from 1.7K vantage points in 164 countries during a one-month period reveals that China hinders access to I2P by poisoning DNS resolutions of the I2P homepage and three reseed servers; SNI-based blocking was detected in Oman and Qatar when accessing the I2P homepage over HTTPS; TCP packet injection was detected in Iran, Oman, Qatar, and Kuwait when visiting the mirror site via HTTP; and explicit block pages were discovered when visiting the mirror site from Oman, Qatar, and Kuwait. Based on these findings, we conclude by discussing potential approaches for improving I2P's resistance to censorship.

2 Background

In this section, we review the VPN Gate ecosystem [73] and the basic operation of the I2P anonymity network [85].

2.1 VPN Gate

VPN Gate is an academic project developed at the University of Tsukuba, Japan [60]. Its core component is a network of distributed VPN vantage points hosted by volunteers from around the world. Unlike commercial VPNs, these VPN vantage points are operated by Internet users who are willing to share their home connection with the primary goal to provide other users with access to the Internet. Volunteers use a software package called SoftEther VPN [59] to turn their personal computer into a VPN server. Other users can then establish VPN connections to these servers using the client component of the same VPN software package.

Advantages. Since VPN Gate's vantage points (VGVPs) are organized and operated by volunteers, they provide three essential benefits that make them a potential resource for measuring censorship at a global scale. First, VGVPs are often located in residential networks, and therefore can help observing filtering policies which may not be observed when measuring from non-residential networks (e.g., data centers). Second, VGVPs provide access to many network locations that are difficult to obtain through commercial VPNs. Our results (§5.2) indeed show that having access to several network locations is important for observing different blocking policies, even within the same country.

Finally, unlike commercial VPNs that often monetize their services by injecting advertisements [49, 51] or even "lying" about their geographical location [78], VGVPs managed by individual operators are unlikely to carry out such illicit practices—this possibility though cannot be excluded, as rogue network relays have been found in Tor [15]. Even if a VGVP is malicious, the chance that it is selected for our measurements is small, given the thousands of available VGVPs. We actually actively looked for and did not observe any malicious JavaScript or ad injection in our measurements.

Limitations. As VGVPs are run by individuals on their personal computers, they cannot guarantee continuous uptime. We can therefore only use them to conduct measurements whenever they are online. Another drawback of using VGVPs is that their availability is susceptible to blocking based on protocol signatures. Local Internet authorities can prevent VGVPs from functioning by filtering the VPN protocols supported by VPN Gate, including L2TP/IPsec, OpenVPN, MS-SSTP, and SSL-VPN (of which OpenVPN is the most dominant protocol). In that case, we will not have access to VGVPs in locations where such filtering policies are applied. VPN Gate mitigates this problem by allowing VGVPs to run on random ports, instead of the default ports of the aforementioned VPN protocols.

2.2 The Invisible Internet Project

I2P is a message-oriented anonymous overlay network comprising relays (also referred to as nodes, routers, or peers) that run the I2P router software to communicate with each other. I2P messages are routed through unidirectional tunnels, which include two tunnel types: inbound and outbound. In the example of Figure 1, each tunnel is illustrated with two hops for simplicity. For a higher anonymity level, these tunnels can be configured to have up to seven hops.

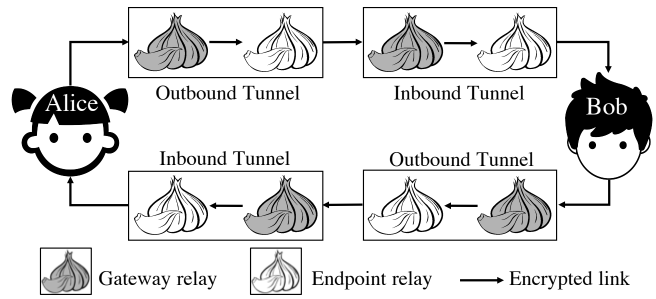

Figure 1: I2P routing mechanism [48].

To communicate with Bob, Alice sends out messages on her outbound tunnels towards the inbound tunnels of Bob. Messages from Bob are sent to Alice in the same way. Alice and Bob learn each other's gateway relay address by querying a network database. The anonymity of both Alice and Bob is preserved since they only know the gateway address, but not the actual address of each other. Note that gateways of inbound tunnels are published, while gateways of outbound tunnels are only known by the relay using them.

The I2P network database (netDb) originates from the Kademlia distributed hash table [54], and plays a vital role in the network, as it is used by relays to look up information of other relays. A newly joined relay learns a portion of the netDb via a bootstrapping process by fetching other relays' information from a group of special relays, called *reseed servers*. Any I2P relay, while communicating with its intended destination, can also route traffic for other relays. In Figure 1, the hops that are selected to form the tunnels are also actual I2P users. While routing messages for Alice and Bob, these hops can also communicate with their intended destinations.

While Tor and I2P share similar properties, there are some operational aspects that differentiate them. Tor traffic is transmitted over TCP, while I2P traffic can be transmitted over either TCP or UDP. Tor has a centralized design with a set of trusted directory authorities keeping track of the network. In contrast, I2P is designed to be a completely decentralized network, with no trusted entity having a complete view of the network.

There are 6.3K Tor routers serving an average of two million concurrent users, estimated from data collected on a daily basis in May, 2019 [6, 72]. There are more than 25K I2P relays, estimated during the same period [61]. While Tor is primarily tailored for latency-sensitive activities (e.g., web browsing) due to bandwidth scarcity [55], I2P is more tolerant towards bandwidth-intensive peer-to-peer (P2P) file sharing applications (e.g., BitTorrent) [74].

3 Methodology

In this section, we present our approach of using the distributed network of VPN Gate servers to conduct opportunistic censorship measurements at a global scale, and approaches to measure the accessibility of different I2P services.

3.1 Vantage Points

From March 10th to April 10th, 2019, we observed 192K VGVPs from 3.5K autonomous systems (ASes) located in 181 countries. Our measurements are conducted in an *opportunistic* fashion, by immediately connecting to a VGVP and running our tests as soon as the node is discovered. There are currently more than 5K VGVPs available at any given time [73], providing us with a redundant amount of vantage points to continuously measure from various network locations. When many VGVPs become available at the same time, we prioritize ones located in region where we have not previously measured.

Due to the high churn rate of VGVPs (§2.1) and the rate limit that we apply (§4), we could conduct a total of 54K measurements from 1.7K ASes in 164 countries, which is still highly comparable to the coverage of other measurement platforms and enough to provide meaningful insights.

3.2 I2P Blocking Detection

To access the I2P anonymity network, users typically go through the following steps:

- Download the router software package from the official I2P website (geti2p.net) or one of its mirror sites, to set up an I2P client.
- The client bootstraps into the network by fetching information about other I2P relays from reseed servers.
- The client can then communicate with its intended destinations via other relays that were previously fetched.

Based on this process, a censor can hinder access to I2P using several blocking techniques, such as domain name blocking [5, 26, 31, 36, 53, 64, 68], TCP packet injection [18, 77], and redirection to block pages [38]. The design of our censorship detection techniques is thus centered around these different blocking techniques.

Domain Name Blocking. From VGVPs, we issue DNS queries to both local and open resolvers,[1] to resolve the domain names of the official I2P homepage (geti2p.net), its mirror site (i2p-projekt.de), and reseed servers. Resolutions of these domain names are vulnerable to DNS-based blocking as they can be seen by any on-path observers, making them an effective vector for censors to block access to I2P as well as other undesired content [5, 26, 31, 53, 64, 68].

By inspecting the traffic captured during these name resolutions and comparing the returned IP addresses with the legitimate ones, we can detect if a DNS response was tampered. More specifically, we aggregate DNS responses returned from known uncensored locations (e.g., the U.S., Canada) to generate a consensus list of legitimate responses, which is then used as ground truth. We also query an "innocuous" domain (example.com), to differentiate between spurious network errors (if any) and filtering events.

As DNS resolutions are a prerequisite to obtain the correct IP address(es) of a domain name, it is often sufficient to conduct DNS-based blocking. Prior work, therefore, has extensively looked at DNS-based blocking [64, 68]. With the introduction of DNS over HTTPS/TLS [43, 45], DNS-based blocking may no longer be an effective filtering channel. Nevertheless, the current design of TLS also exposes visited domain names in the Server Name Indication (SNI) extension [46]. SNI provides a second channel for on-path observers to monitor HTTPS-based sites, and thus it can be used to interrupt connections to censored destinations [35, 36].

To also examine whether SNI-based blocking is being used by censors in light of encrypted DNS traffic, we connect to the legitimate IP address of the I2P official homepage [2] over the VPN tunnel of VGVPs, and then monitor if the connection was interrupted during the TLS handshake.

TCP Packet Injection. The injection of TCP RST (reset) or FIN (finish) packets is another common method for blocking connections to censored websites [58] and services [27]. To observe this filtering technique, it is desirable to capture and analyze network traffic while establishing connections to tested destinations. At the same time with i) crawling the I2P homepage and its mirrors, and ii) establishing TCP connections to the reseed servers and five I2P relays (set up by us—see §4), we also capture network traffic passing through the VPN interface between our testing machines and VGVPs. The captured network traffic is then analyzed to see if there was any injection interfering with our connections.

Block Pages. Block pages are a form of overt censorship in which censors explicitly let users know about their blocking intention [38]. Block pages can be delivered through various methods. A censor can poison the DNS resolution of censored websites to route users to the block page. We observe this type of blocking from an institutional network in South Korea (see §5.1). Another method is to interfere with the TCP stream to redirect users to the block page, which we observe in Oman, Qatar, and Kuwait (see §5.3). As the I2P official site does not change much during our measurement period, we could simply compare the HTML body of the legitimate site with those fetched over VGVPs to detect block pages. For future reference, when crawling the I2P site and its mirror, we also capture a screenshot of any delivered block page.

[1] We use public DNS resolvers, including Google's 8.8.8.8 and 8.8.4.4, Cloudflare's 1.1.1.1 and 1.0.0.1, and Cisco Umbrella OpenDNS's 208.67.222.222 and 208.67.220.220.

[2] Currently, only the official homepage is served over HTTPS. Mirror sites are still served over HTTP.

4 Ethical Considerations

As Internet censorship is often politically motivated [19, 40], measurements involving volunteer-operated devices need to be conducted in a careful manner [4, 50, 69]. While there are some commercial VPN services that also provide access to residential networks (e.g., Geosurf [37], Hola [1], Luminati [2]), there have been reports of illicit behaviors by some of these VPNs [56], making them inappropriate to use for academic purposes. We instead opt to conduct our measurements using VPN Gate's volunteer-run nodes for several reasons.

VPN Gate is an academic project and does not have any motivation to monetize its service like commercial VPN providers [49, 51]. To become a VPN server, the SoftEther VPN software requires an operator to manually go through a process with repeated warning messages about the associated risks of joining the VPN Gate research network [44]. We therefore expect that VGVP operators fully understand the potential issues of sharing their connection.

The VPN Gate software, as well as the infrastructure at the University of Tsukuba, both have logging mechanisms to assist VPN operators in case of complaints or disputes. Although log retention can be a security and privacy risk for VPN users, these logs serve as an anti-abuse policy used by the project to protect its volunteers. The University of Tsukuba, and the VPN Gate project in particular, operate under Japan laws, and thus will only provide logs if there are valid reasons to obtain them by authorized entities. Foreign authorities who want these logs will have to adhere to Japan laws and request them via the Minister for Foreign Affairs [66].

Our study of the I2P anonymity network, which comprises thousands of users, must be performed in a responsible manner that both respects user privacy [69, 84] and ensures that our measurements do not interfere with the normal operation of the I2P network [47]. We therefore apply an average rate limit of three measurements per minute to make sure that our experiments do not saturate any I2P or VPN Gate services, thus affecting other users.

Our measurements involve connecting to other I2P relays whose IP address(es) may be considered as sensitive information under certain circumstances, as they could be used to identify individuals. To prevent this privacy risk, we set up our own I2P relays for this study and only test the connectivity between VGVPs and these relays. Setting up our own relays provides several benefits. First, they help to avoid any privacy risks associated with using other relays. Second, they improve the accuracy of our measurements, since I2P is a dynamic network in which relays join and leave the network frequently. The high churn rate of relays may negatively affect our observations. Finally, measurements on our own I2P relays will not interrupt normal usage of other relays in the network.

More importantly, the I2P community has published a set of guidelines [47] for conducting studies on the I2P network, to which we strictly adhered. In accordance with these guidelines, we contacted the I2P team to discuss the purposes of our measurements. While capturing the network traffic of our measurements, we do not capture any traffic of other I2P or VPN Gate users. Particularly, we only "listen" for traffic passing through the VPN interface between our testing machines and VGVPs. This network traffic thus contains only packets generated by our tests, as discussed in §3.2.

5 Data Analysis

Between March 10th to April 10th, 2019, we conducted a total of 54K measurements from 1.7K ASes in 164 countries, and detected I2P blocking activities in five countries: China, Iran, Oman, Qatar, and Kuwait. In the following, we discuss in detail the different types of blocking we observed. A summary of our findings is provided in Table 2 in the appendix.

5.1 Domain Name Blocking

DNS-based Blocking. China is dominant in terms of DNS-based blocking events across all VGVPs used. Based on the method described in §3.2, we detect DNS poisoning attempts when resolving domains of the I2P homepage and reseed servers. While open resolvers are often used by Internet users to bypass local censorship, we find that China's Great Firewall (GFW) [53, 82] also poisons DNS responses from our selected open resolvers when resolving censored domains. However, we could obtain the correct DNS records for the "innocuous" domain (i.e., example.com), which means that despite monitoring all DNS resolutions passing by, the GFW does not block access to open resolvers and only poisons responses for censored domains.

Table 1 lists the ASes from which we detect poisoned DNS responses. The second column shows censored domains. The third column shows /24 subnets that are most frequently abused by the GFW to inject falsified DNS responses. While Pakistan, Syria, and Iran poison DNS responses with NXDOMAIN [11, 14, 57] or reserved local IP addresses [10], making them easier to distinguish, China often falsifies DNS responses with public IP addresses belong to other non-Chinese organizations [12, 31, 53, 64, 82].

Of these abused IP addresses, several were observed by previous studies. Similar to an initial observation by Lowe et al. [53], we also observed 64.33.88.161, 203.161.230.171, and 4.36.66.178 among the most abused addresses. Similar to Pearce et al. [64] and Farnan et al. [31], 8.7.198.45, 59.24.3.173, and 78.16.49.15 were also observed although they are not within the group of most abused addresses. In addition to those seen by previous work, to our surprise, we found many new abused IP addresses, most of which belong to Facebook and SoftLayer.

Although the IP addresses that are used to poison DNS responses are similar across most ASes, showing a centralized

Chinese ASes	Censored domains	Most abused /24 subnets
AS134762, AS17816, AS4134, AS4808 AS4812, AS4837, AS56005, AS56040 AS56041, AS56042, AS56046, AS9808(*)	geti2p.net, i2p-projekt.de(*) reseed.i2p-projekt.de, netdb.i2p2.no i2p.mooo.com, i2p.novg.net(*)	64.33.88.0, 203.161.230.0, 31.13.72.0, 4.36.66.0, 74.86.151.0, 74.86.12.0, 69.63.184.0, 69.171.229.0, 66.220.152.0, 66.220.149.0, 31.13.84.0

Table 1: Censored domains in China and top IP addresses that are most frequently abused for poisoning DNS responses.

list of IPs that are being abused by the GFW, the block list of domains and blocking mechanisms seem to be implemented differently at different network locations. For instance, in addition to four domains poisoned at most ASes in China, we also observed DNS poisoning attempts at AS9808 (Guangdong Mobile Communication) when resolving *i2p-projekt.de* and *i2p.novg.net*. Analyzing packets captured from this AS, we notice that the way poisoned responses were crafted is different from other ASes. More specifically, while poisoned responses at other locations contain only the falsified IP addresses shown in Table 1, poisoned responses at AS9808 also have an additional resource record of a loopback IP address (i.e, 127.0.0.1). Nevertheless, this phenomenon could also happen due to implementation bugs of the GFW, as it only occurred sporadically but not consistently during the period of our study. Previous work has shown that the GFW may not function as desired sometimes [30].

In conclusion, our measurements show that the I2P homepage is censored by DNS-based blocking, while its mirror is still accessible from most network locations in China. Of the ten reseed servers that were active during our measurement period, three were consistently blocked by DNS poisoning. Our observations align with findings of earlier studies. We previously conducted active measurements from China to test the reachability of reseed servers and found that some of them were still accessible [41]. Moreover, our I2P metrics site [61] also shows a consistent number of Chinese relays during our measurement period. A recent study by Ververis et al. [76] also shows that the I2P Android App is still available for download from the Tencent App Store despite the removal of many other censorship circumvention applications.

SNI-based Blocking. As mentioned in §3.2, we also investigate whether censors employ SNI-based blocking together with DNS-based blocking, as these are the two main channels where visited domains are exposed. Surprisingly, we could successfully fetch the official I2P homepage from the network locations in China, where the website was previously blocked by the GFW's DNS poisoning. Although OONI recently reported that China does employ SNI-based blocking together with DNS-based blocking to censor all domains belonging to Wikipedia [70], our findings show that this technique is not fully employed for all censored domains. In other words, the GFW may apply different blocking techniques against different domains and services.

Institutional Filtering and Leakage of DNS Injection. Apart from poisoned responses observed in China, we also detect DNS-based blocking at AS38676, AS9848, and AS1781 in Korea. For AS1781, which is managed by the Korea Advanced Institute of Science and Technology, poisoned DNS responses contain only one static IP addresses (143.248.4.221). Upon visiting the webpage hosted under this IP address, it becomes obvious that the Institute has deployed a firewall to filter anonymity services. Note that filtering activities observed at institutional networks should be carefully analyzed and not characterized as national-level filtering. Of the 1.7K networks we have access to, there are 64 institutional networks in 17 countries. However, after excluding VGVPs from these networks, we still have access to other VGVPs located in residential networks in these 17 countries.

Next, we notice that the pattern of poisoned responses in AS38676 and AS9848 is not consistent. More specifically, we only observed poisoned responses sporadically on some days, while we could obtain correct responses on some other days. Further investigation from the captured network traffic shows that poisoned responses were only injected when querying the open resolvers but not local resolvers. Therefore, it is clear that operators of these two networks do not block access to I2P. Moreover, the set of falsified IP addresses is similar to those observed in China, as shown in Table 1. This is likely the case of China's censorship leakage because China inspects and censors both egress and ingress network traffic passing through the GFW. Due to the geographical proximity of Korea and China, it is likely that our DNS queries sent from Korea to open resolvers passed through China's network, and thus got poisoned [9, 22].

5.2 TCP Packet Injection

During our measurement period, we detected injection of TCP packets while visiting the I2P official homepage and its mirror site in four countries. More specifically, we find that the I2P mirror site is blocked in Iran, while the official website is still accessible over HTTPS. Analyzing the captured network traffic, we could detect TCP packets injected immediately after the HTTP GET request containing the hostname was sent out. The injected TCP packets contain HTTP 403 Forbidden, thus disrupting the normal connection.

We also found injected TCP packets from VGVPs located in Oman and Qatar. These two censors use the same blocking techniques to prevent access to both official and mirror sites. When connecting to the HTTP mirror site, TCP packets were injected immediately after the HTTP GET request, redirecting users to block pages (see §5.3). When connecting to the official site (over HTTPS), SNI-based blocking is used to interrupt the connection. More specifically, although the TCP handshake between geti2p.net and our VGVPs in these two countries could successfully complete, immediately after the TLS client-hello message was sent out, a TCP RST packet was then injected, terminating the TCP stream.

Similar blocking activities with Iran were also detected in Kuwait. More specifically, the I2P homepage is still accessible, while its mirror site is blocked by means of TCP packet injection, redirecting users to a block page (see §5.3). However, unlike Iran, Oman, and Qatar, where we observe filtering events in many network locations, we consistently observe blocking activities only at AS47589 (Kuwait Telecommunication Company), while all I2P services could be accessed normally from other network locations in this country.

5.3 Block Pages

Although explicit block pages can be delivered to censored users through either DNS poisoning or TCP packet injection, as discussed above, we mostly observed block pages at a national level being delivered through TCP packet injection. Comparing the HTML body of the legitimate official homepage and the HTML fetched via VGVPs, we could simply pinpoint block pages returned by censors and detect explicit block pages in Oman, Qatar, and Kuwait.

Based on the content of the delivered message on each block page (some examples are provided in Appendix A), it is clear that blocking access to I2P is required by the state law in each of these three countries. Note that although we observed the same block pages in all network locations in Oman and Qatar, of six networks in Kuwait (AS3225, AS42961, AS9155, AS6412, AS196921, and AS47589) from which we conducted our measurements, we only detected censorship in AS47589. The block page explicitly explains the site is restricted under Internet services law in the State of Kuwait. This observation shows that there is always region-to-region and ISP-to-ISP variation, thus necessitating comprehensive measurements to be conducted from several network locations to accurately attribute censorship (i.e., at a local or national level).

5.4 Comparison with other Platforms

Among currently active censorship measurement platforms, OONI [32] is comparable to ours in terms of coverage, with about 160 countries and 2K network locations as of 2019. ICLab [58] is also similar to ours in terms of censorship detection techniques and the design decision of using VPN vantage points to measure network filtering.

OONI provides installation packages for several platforms, including Raspberry Pi, OS X, Linux, Google Play, F-Droid, and Apple's App Store, making it easier for testers from around the world to download the package and run it. OONI, however, does not have full control over the measurements conducted by its volunteers. These measurements, therefore, may be interrupted by unexpected spurious network connectivity issues at the testing client side, making the collected data unusable or even unreliable in some cases [83].

We analyzed OONI data collected during the same study period with ours to examine if OONI also detected similar blocking events. While the domain name of the I2P homepage has been added to the global test list of OONI since February, 2019 [16], we could not find any OONI tests of the I2P website conducted from the countries in which we detected I2P censorship (§5), except for one test conducted in Iran. Upon closer inspection of this test attempt, conducted by an OONI volunteer in Iran [3], we found that the test could not provide reliable data due to a control failure.

We have also collaborated with the authors of ICLab [58] to use their platform for conducting I2P censorship measurements. However, we did not detect any filtering activities from measurement data obtained by ICLab. Understandably, ICLab has a more limited coverage of 62 countries, as of December 2018. Among the five countries in which we detected I2P blocking events, IClab only has vantage points in Iran and China. However, connections to them were very intermittent, thus could not provide us with reliable data. This is one of the advantages of our proposed infrastructure compared with commercial VPN services, as gaining access to networks in countries with less freedom of expression can be challenging.

6 Related Work

Many studies have conducted censorship measurements in separate countries. The GFW of China has been extensively studied due to its significance [17, 27, 30, 63, 80, 81]. Some other well-known censors, including Iran [8, 10], India [83], Pakistan [52, 57], Syria [14], Yemen [21], Egypt, and Libya [20], have also been studied. Throughout our study, we investigated the blocking situation of different I2P services in many countries. In addition to those that have been studied previously, our study have discovered explicit blockage in three more countries: Oman, Qatar, and Kuwait.

ICLab [58], OONI [32], Quack [75], Iris [64], and Satellite [68] are currently active platforms that are capable of measuring censorship at a global scale. Despite sharing a similar goal with us, each platform has its own drawbacks which can be complemented by our proposed measurement infrastructure. While the design of ICLab is similar to ours, it is challenging for the platform to obtain reliable vantage points from commercial VPN providers in some countries of interest where we have discovered I2P blocking activities. Although OONI is widely known for its worldwide censorship measurement activities, Yadav et al. showed that this platform can result in some inaccuracy [83].

Satellite-Iris [13], a combination between two prior works (Satellite [68] and Iris [64]), uses open DNS resolvers in the IPv4 space to detect DNS-based network filtering. With a similar design that uses Zmap [28] to probe the whole IPv4 space to detect open servers, Quack [75] scans for public echo servers and takes advantage of these servers to measure censorship. The primary goal of Quack is to detect censorship of websites, but does not send or receive actual HTTP(S) packets. The platform, instead, crafts packets that mimic HTTP(S) requests, which the echo server will reflect back to the testing client. Nonetheless, Quack's authors have acknowledged the possibility of false negatives when the censor only looks for HTTP(S) traffic on the usual ports (80 and 443) since the echo protocol operates over port 7 [65].

7 Discussion

We have introduced an infrastructure that can remedy the common challenge faced by current Internet censorship measurement platforms, which is the trade-off between depth of measurement and breadth of coverage. The infrastructure is built on top of a network of distributed VPN servers, providing us with not only a redundant amount of vantage points around the world, but also the flexibility of the VPN technology in applying different testing techniques to measure network filtering activities at a global scale.

Due to the limitations discussed in §2, however, we do not consider the proposed infrastructure as a replacement of existing measurement platforms. Instead, it should be used as a complementary tool for conducting additional measurements from locations in which current platforms cannot have access to, providing more data to analyze and improve the accuracy of censorship measurement results. For example, OONI volunteers can connect to VGVPs and run tests to increase the coverage and accuracy of OONI's data. Similarly, ICLab could integrate VPN Gate's OpenVPN configuration files into its measurement platform to increase the coverage of both network locations and countries of interest.

Our findings show that the most dominant filtering technique is based on domain names. Currently, visited domain names can be observed in two channels: DNS queries and the SNI extension (if HTTPS is supported), making them effective filtering vectors for on-path observers. While DNS over HTTPS/TLS [43,45] and ESNI [67] are still being developed and have not been widely adopted yet, we believe that domain name blocking will no longer be an effective technique once these new techniques become standardized.[3]

Assuming a future Internet with all traffic encrypted, it is likely that censors will switch to employing IP-based blocking. Our measurement data shows that the I2P official homepage, its mirror site, and reseed servers are hosted on static IP addresses. As a result, it is trivial for a censor to block access to these services by blacklisting all associated hosting IP addresses. In order to cope with this problem, operators of these domain names should consider hosting them on dynamic IP address(es) that may also host many other websites, to discourage censors from conducting IP-based blocking due to the cost of collateral damage of blocking many "innocuous" co-hosted sites.

The I2P developers have foreseen a scenario in which all reseed servers get blocked, thus preventing new relays from joining the network. They therefore have created a function in the I2P router software for manual reseeding. Using this function, any active I2P relay can manually extract information of a set of its known active relays and share it with censored relays that do not have access to any reseed servers. Under this situation, a censor who wants to prevent local users from accessing the I2P network will have to harvest all IP addresses of active I2P relays and block them all. While in our previous work we showed that this harvesting attack could be conducted at a relatively low cost [41], we did not observe any such blocking activities while conducting connectivity tests between VGVPs and our own I2P relays.

8 Conclusion

Over a one-month period, we used a network of VPN servers distributed across 164 countries to conduct 54K measurements with the goal of investigating the blocking of I2P at a global scale. We find that several I2P services (e.g., the homepage, its mirror site, and a subset of reseed servers) are being blocked using different filtering techniques in five countries.

China blocks access to the I2P official homepage and a part of reseed servers by poisoning DNS resolutions. Iran interrupts connections to the mirror site by injecting forged TCP packets containing HTTP 403 Forbidden code. SNI-based blocking was detected when visiting the I2P official homepage over HTTPS in Oman and Qatar, while explicit block pages were also detected when visiting the mirror site via HTTP. Block page redirection was also detected in the network of Kuwait Telecommunication Company when visiting the I2P mirror site. Finally, we discussed potential approaches to help I2P tackle censorship based on the above findings.

Acknowledgments

We would like to thank our shepherd, Masashi Crete-Nishihata, and all of the anonymous reviewers for their thorough feedback on earlier drafts of this paper. We also thank Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill from the ICLab team for collaborating with us to run measurements to test I2P accessibility on their platform, and for constructive discussions. We also thank Vasilis Ververis, Marios Isaakidis, and Valentin Weber for helpful conversations and early sharing of their app store censorship study.

This research was supported in part by the Open Technology Fund under an Information Controls Fellowship. The opinions in this paper are those of the authors and do not necessarily reflect the opinions of the sponsor.

[3] Unless users are forced to use the DNS resolvers provided by their local Internet authority, and they cannot use any other third-party open DNS resolvers that support DNS over HTTPS/TLS.

References

[1] Hola VPN: Unblock any website. https://hola.org.

[2] Luminati proxy service. https://luminati.io.

[3] OONI test of geti2p.net from Iran. http://bit.ly/OONI-I2P-Measurement-in-Iran.

[4] Communications Disruption & Censorship under International Law: History Lessons. In *2nd USENIX Workshop on Free and Open Communications on the Internet*, Bellevue, WA, 2012. USENIX.

[5] Towards a Comprehensive Picture of the Great Firewall's DNS Censorship. In *4th USENIX Workshop on Free and Open Communications on the Internet*, San Diego, CA, 2014. USENIX Association.

[6] Tor Metrics, 2018. https://metrics.torproject.org/userstats-relay-country.html?start=2019-05-01&end=2019-05-20.

[7] Nicholas Aase, Jedidiah R. Crandall, Alvaro Diaz, Jeffrey Knockel, Jorge Ocana Molinero, Jared Saia, Dan Wallach, and Tao Zhu. Whiskey, Weed, and Wukan on the World Wide Web: On Measuring Censors' Resources and Motivations. In *2nd USENIX Workshop on Free and Open Communications on the Internet*, Bellevue, WA, 2012. USENIX.

[8] Collin Anderson. Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran. 2013.

[9] Anonymous. The Collateral Damage of Internet Censorship by DNS Injection. *SIGCOMM Computer Communication Review*, 42(3):21–27, 6 2012.

[10] Simurgh Aryan, Homa Aryan, and J. Alex Halderman. Internet Censorship in Iran: A First Look. In *3rd USENIX Workshop on Free and Open Communications on the Internet*, Washington, D.C., 2013. USENIX.

[11] S. Bortzmeyer and S. Huque. NXDOMAIN: There Really Is Nothing Underneath. RFC 8020, IETF, 2016.

[12] Martin A Brown, Doug Madory, Alin Popescu, and Earl Zmijewski. DNS Tampering and Root Servers.

[13] Censored Planet: Satellite and Iris. Available at https://censoredplanet.org/projects/satellite.

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

[15] Sambuddho Chakravarty, Georgios Portokalidis, Michalis Polychronakis, and Angelos D. Keromytis. Detecting Traffic Snooping in Tor Using Decoys. In *Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection (RAID)*, pages 222–241, September 2011.

[16] Citizen Lab Block List. Add geti2p.net to the global test list. Available at http://bit.ly/OONI-added-to-Citizenlab_blocklist.

[17] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson. Ignoring the Great Firewall of China. In *Privacy Enhancing Technologies*, volume 4258 of *LNCS*, pages 20–35, Berlin, Heidelberg, 2006. Springer.

[18] Jedidiah R. Crandall, Daniel Zinn, Michael Byrd, Earl Barr, and Rich East. ConceptDoppler: A Weather Tracker for Internet Censorship. In *Computer and Communications Security*, pages 352–365, New York, 2007.

[19] M. Crete-Nishihata, R. Deibert, and A. Senft. Not by Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls. *IEEE Internet Computing*, 17(3):34–41, May 2013.

[20] Alberto Dainotti, Claudio Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russo, and Antonio Pescape. Analysis of Country-Wide Internet Outages Caused by Censorship. *IEEE/ACM Transactions on Networking*, 2013.

[21] Jakub Dalek, Ronald Deibert, Sarah McKune, Phillipa Gill, Naser Noor, and Adam Senft. Information Controls During Military Operations: The Case of Yemen During the 2015 Political and Armed Conflict. Technical report.

[22] Chris C Demchak and Yuval Shavitt. China's Maxim–Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking. *Military Cyber Affairs*, 3(1):7, 2018.

[23] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. In *Proceedings of the 13th USENIX Security Symposium*, pages 303–319, August 2004.

[24] Roger Dingledine. The Free Haven Project: Design and Deployment of an Anonymous Secure Data Haven. Master's thesis, MIT, Dept. of Electrical Engineering and Computer Science, 2000.

[25] Roger Dingledine, Michael J. Freedman, and David Molnar. The Free Haven Project: Distributed Anonymous Storage Service. In *International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability*, pages 67–95, Berlin, Heidelberg, 2001. Springer-Verlag.

[26] Hai-Xin Duan, Nicholas Weaver, Zengzhi Zhao, Meng Hu, Jinjin Liang, Jian Jiang, Kang Li, and Vern Paxson. Hold-On: Protecting Against On-Path DNS Poisoning. In *Proceedings of the Conference on Securing and Trusting Internet Names (SATIN)*, 2012.

[27] Arun Dunna, Ciarán O'Brien, and Phillipa Gill. Analyzing China's Blocking of Unpublished Tor Bridges. In *8th USENIX Workshop on Free and Open Communications on the Internet*, Baltimore, MD, 2018. USENIX.

[28] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. ZMap: Fast Internet-wide Scanning and Its Security Applications. In *the 22nd USENIX Security Symposium (USENIX Security 13)*, pages 605–620, Washington, D.C., 2013. USENIX.

[29] Roya Ensafi, David Fifield, Philipp Winter, Nick Feamster, Nicholas Weaver, and Vern Paxson. Examining How the Great Firewall Discovers Hidden Circumvention Servers. In *Conference on Internet Measurement Conference*, pages 445–458, New York, USA, 2015.

[30] Roya Ensafi, Philipp Winter, Abdullah Mueen, and Jedidiah R Crandall. Analyzing the Great Firewall of China over Space and Time. *Proceedings on Privacy Enhancing Technologies*, 2015(1):61–76, 2015.

[31] Oliver Farnan, Alexander Darer, and Joss Wright. Poisoning the Well: Exploring the Great Firewall's Poisoned DNS Responses. In *Workshop on Privacy in the Electronic Society*, pages 95–98, New York, 2016. ACM.

[32] Arturo Filasto and Jacob Appelbaum. OONI: Open Observatory of Network Interference. In *2nd USENIX Workshop on Free and Open Communications on the Internet*, 2012.

[33] Michael J Freedman. Design and Analysis of an Anonymous Communication Channel for the Free Haven Project.

[34] Freedom House. Freedom on the Net 2018: The Rise Of Digital Authoritarianism, 2018. Available at https://freedomhouse.org/report/freedom-net/freedom-net-2018.

[35] Sergey Frolov and Eric Wustrow. The use of TLS in Censorship Circumvention. In *Network and Distributed System Security*. The Internet Society, 2019.

[36] Sergiu Gatlan. South Korea is Censoring the Internet by Snooping on SNI Traffic, 2019. Available at https://www.bleepingcomputer.com/news/security/south-korea-is-censoring-the-internet-by-snooping-on-sni-traffic/.

[37] Geosurf. Geosurf: Residential and data center proxy network. Available at https://www.geosurf.com.

[38] Phillipa Gill, Masashi Crete-Nishihata, Jakub Dalek, Sharon Goldberg, Adam Senft, and Greg Wiseman. Characterizing Web Censorship Worldwide: Another Look at the OpenNet Initiative Data. *ACM Transactions on the Web*, 9(1), 2015.

[39] David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. Hiding Routing Information. In Ross Anderson, editor, *Information Hiding*, pages 137–150, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[40] Seth Hardy, Masashi Crete-Nishihata, Katharine Kleemola, Adam Senft, Byron Sonne, Greg Wiseman, Phillipa Gill, and Ronald J. Deibert. Targeted Threat Index: Characterizing and Quantifying Politically-Motivated Targeted Malware. In *23rd USENIX Security Symposium*, pages 527–541. USENIX, 2014.

[41] Nguyen Phong Hoang, Panagiotis Kintis, Manos Antonakakis, and Michalis Polychronakis. An Empirical Study of the I2P Anonymity Network and Its Censorship Resistance. In *Internet Measurement Conference 2018*, pages 379–392, New York, NY, USA, 2018. ACM.

[42] Nguyen Phong Hoang and Davar Pishva. Anonymous Communication and Its Importance in Social Networking. In *16th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2 2014.

[43] P. Hoffman and P. McManus. DNS Queries over HTTPS (DoH). RFC 8484, IETF, October 2018.

[44] How to Enable or Disable the VPN Relay Function on VPN Gate Client? Available at https://www.vpngate.net/en/join_client.aspx.

[45] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman. Specification for DNS over Transport Layer Security (TLS). RFC 7858, IETF, May 2016.

[46] Huawei. Transport layer security (TLS) extensions: Server name indication. RFC 6066, IETF, January 2011.

[47] I2P Homepage. Academic Research Guidelines. Available at https://geti2p.net/en/research.

[48] I2P Homepage. A Gentle Introduction to How I2P Works, 2017. Available at https://geti2p.net/en/docs/how/intro.

[49] Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar, and Vern Paxson. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. In *Internet Measurement Conference*, pages 349–364, New York, NY, USA, 2016. ACM.

[50] Ben Jones, Roya Ensafi, Nick Feamster, Vern Paxson, and Nick Weaver. Ethical Concerns for Censorship Measurement. In *Proceedings of the 2015 ACM SIGCOMM Workshop on Ethics in Networked Systems Research*, pages 17–19, New York, NY, USA, 2015. ACM.

[51] Mohammad Taha Khan, Joe DeBlasio, Geoffrey M. Voelker, Alex C. Snoeren, Chris Kanich, and Narseo Vallina-Rodriguez. An Empirical Analysis of the Commercial VPN Ecosystem. In *Proceedings of the Internet Measurement Conference 2018*, IMC '18, pages 443–456, New York, NY, USA, 2018. ACM.

[52] Sheharbano Khattak, Mobin Javed, Syed Ali Khayam, Zartash Afzal Uzmi, and Vern Paxson. A Look at the Consequences of Internet Censorship Through an ISP Lens. In *Internet Measurement Conference*, pages 271–284, New York, 2014. ACM.

[53] Graham Lowe, Patrick Winters, and Michael L Marcus. The Great DNS Wall of China. 2007.

[54] Petar Maymounkov and D Mazieres. Kademlia: A Peer-to-Peer Information System Based on the XOR Metric. In *First International Workshop on Peer-to-Peer Systems*, pages 53–65, 2002.

[55] Damon McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. Shining Light in Dark Places: Understanding the Tor Network. In Nikita Borisov and Ian Goldberg, editors, *Privacy Enhancing Technologies*, pages 63–76, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[56] Xianghang Mi, Ying Liu, Xuan Feng, Xiaojing Liao, Baojun Liu, XiaoFeng Wang, Feng Qian, Zhou Li, Sumayah Alrwais, and Limin Sun. Resident Evil: Understanding Residential IP Proxy as a Dark Service. In *Symposium on Security and Privacy*, pages 170–186. IEEE, 2019.

[57] Zubair Nabi. The Anatomy of Web Censorship in Pakistan. In *3nd USENIX Workshop on Free and Open Communications on the Internet*, Berkeley, CA, 2013.

[58] Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, and Phillipa Gill. ICLab: A Global, Longitudinal Internet Censorship Measurement Platform. In *IEEE Symposium on Security and Privacy*, May 2020.

[59] Daiyuu Nobori. Virtual Ethernet System and Tunneling Communication with SoftEther. *The 45th Programming Symposium of Information Processing Society of Japan*, pages 147–158, Jan 2004.

[60] Daiyuu Nobori and Yasushi Shinjo. VPN Gate: A Volunteer-Organized Public VPN Relay System with Blocking Resistance for Bypassing Government Censorship Firewalls. In *Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation*, pages 229–241, Seattle, WA, 2014. USENIX.

[61] NP. Hoang. I2P Metrics Portal - Router Population. Available at https://i2p-metrics.np-tokumei.net/network-size.

[62] Palko Karasz. What Is Telegram, and Why Are Iran and Russia Trying to Ban It? The New York Times, 2018-05-02. Available at https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html.

[63] Jong Chun Park and Jedidiah R. Crandall. Empirical Study of a National-scale Distributed Intrusion Detection System: Backbone-level Filtering of HTML Responses in China. In *Distributed Computing Systems*, pages 315–326, Piscataway, NJ, 2010. IEEE.

[64] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. Global Measurement of DNS Manipulation. In *26th USENIX Security Symposium*, 2017.

[65] J. Postel. Echo protocol. RFC 862, IETF, May 1983.

[66] Procedure to request for logs from the VPN Gate project. Available in Japanese at https://www.vpngate.net/ja/about_abuse.aspx.

[67] E. Rescorla, K. Oku, N. Sullivan, and C. Wood. Encrypted Server Name Indication for TLS 1.3. Internet draft, IETF, March 2019.

[68] Will Scott, Thomas Anderson, Tadayoshi Kohno, and Arvind Krishnamurthy. Satellite: Joint Analysis of CDNs and Network-Level Interference. In *USENIX Annual Technical Conference*, 2016.

[69] Douglas C. Sicker, Paul Ohm, and Dirk Grunwald. Legal Issues Surrounding Monitoring During Network Research. In *Conference on Internet Measurement*, pages 141–148, New York, NY, USA, 2007. ACM.

[70] Sukhbir Singh, Arturo Filastò, and Maria Xynou. China is now blocking all language editions of Wikipedia, 2019. Available at https://ooni.torproject.org/post/2019-china-wikipedia-blocking/.

[71] P. F. Syverson, D. M. Goldschlag, and M. G. Reed. Anonymous Connections and Onion Routing. In *IEEE Symposium on Security and Privacy*, May 1997.

[72] The Tor Project. Questions and answers about user statistics. Available at https://gitweb.torproject.org/metrics-web.git/tree/src/main/resources/doc/users-q-and-a.txt.

[73] The VPN Gate Project. https://www.vpngate.net.

[74] Juan Pablo Timpanaro, Chrisment Isabelle, and Festor Olivier. *Monitoring the I2P network*. PhD thesis, INRIA, 2011.

[75] Ben VanderSloot, Allison McDonald, Will Scott, J. Alex Halderman, and Roya Ensafi. Quack: Scalable Remote Measurement of Application-Layer Censorship. In *USENIX Security Symposium*, 2018.

[76] Vasilis Ververis, Marios Isaakidis, Valentin Weber, and Benjamin Fabian. Shedding Light on Mobile App Store Censorship. In *Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization*, UMAP'19 Adjunct, pages 193–198, New York, NY, USA, 2019. ACM.

[77] Nicholas Weaver, Robin Sommer, and Vern Paxson. Detecting Forged TCP Reset Packets. In *Network and Distributed System Security*. Internet Society, 2009.

[78] Zachary Weinberg, Shinyoung Cho, Nicolas Christin, Vyas Sekar, and Phillipa Gill. How to Catch when Proxies Lie: Verifying the Physical Locations of Network Proxies with Active Geolocation. In *Proceedings of the Internet Measurement Conference 2018*, IMC '18, pages 203–217, New York, NY, USA, 2018. ACM.

[79] P Winter and S Lindskog. How the Great Firewall of China is Blocking Tor. In *2nd USENIX Workshop on Free and Open Communications on the Internet*. USENIX, 2012.

[80] Joss Wright. Regional Variation in Chinese Internet Filtering. *Information, Communication & Society*, 17(1):121–141, 2014.

[81] Xueyang Xu, Z. Morley Mao, and J. Alex Halderman. Internet Censorship in China: Where Does the Filtering Occur? In *Passive and Active Measurement*, volume 6579 of *LNCS*, pages 133–142. Springer, 2011.

[82] Young Xu. Deconstructing the Great Firewall of China. Technical report, Thousand Eyes, 2016.

[83] Tarun Kumar Yadav, Akshat Sinha, Devashish Gosain, Piyush Kumar Sharma, and Sambuddho Chakravarty. Where The Light Gets In: Analyzing Web Censorship Mechanisms in India. In *Internet Measurement Conference*, pages 252–264, New York, NY, USA, 2018. ACM.

[84] Bendert Zevenbergen, Ian Brown, Joss Wright, and David Erdos. Ethical Privacy Guidelines for Mobile Connectivity Measurements. *SSRN Electronic Journal*, Jan 2013.

[85] zzz (Pseudonym) and Lars Schimmer. Peer Profiling and Selection in the I2P Anonymous Network. In *Proceedings of PET-CON*, pages 59–70, March 2009.

A Appendix

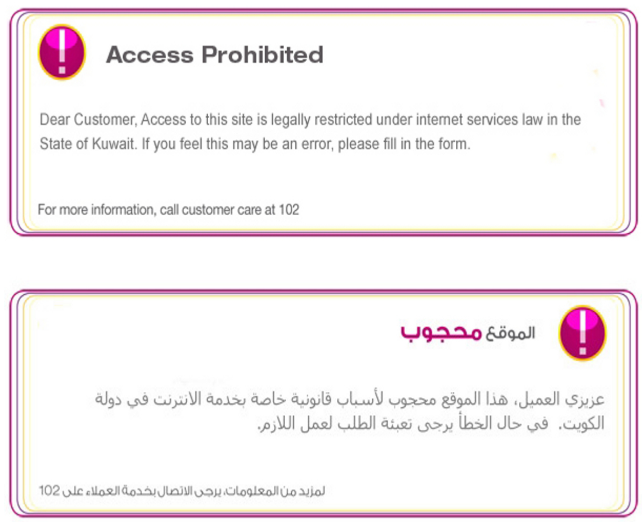

Figure 2: Example block page from Kuwait.

Figure 3: Example block page from Qatar.

Important Notice

تم حجب هذا الموقع أو جزء منه بسبب تعارضه مع قواعد السلوك في سلطنة عمان. وقد يكون محتواه إما مسيئا أو مهينا أو فاحشا أو غير أخلاقي أو
يروج معلومات مضللة أو احتيالية أو مواد غير قانونية. إذا كنت تعتقد أن الموقع الإلكتروني الذي تحاول الوصول إليه لا يحتوي أي من هذه المحتويات،
يرجى تعبئة الاستمارة التالية:

This website or part thereof is blocked due to its breaching of the decency code of conduct of Sultanate of Oman. It has been found to either be abusive, offensive, obscene, immoral or promoting misleading or fraudulent information or illegal material. If you believe that the website you are trying to access does not contain any such content, please submit the below form:

Website Access Blocking/Unblocking Request Form

All fields are mandatory * | جميع الحقول مطلوبة *

Full Name * | الأسم بالكامل*

Contact Number * | رقم الهاتف *

Email Address * | العنوان البريدي *

URL of the WebSite * | الرابط الإلكتروني للموقع *

Justifications & Comments * | المبررات والتعليقات *

Figure 4: Example block page from Oman.

Country	Domain-name-based blocking		TCP packet injection	Block page
	DNS	SNI		
China	geti2p.net reseed.i2p-projekt.de netdb.i2p2.no i2p.mooo.com	N/A	N/A	N/A
Iran	N/A	N/A	i2p-projekt.de	N/A
Oman	N/A	geti2p.net	geti2p.net i2p-projekt.de	i2p-projekt.de
Qatar	N/A	geti2p.net	geti2p.net i2p-projekt.de	i2p-projekt.de
Kuwait	N/A	N/A	i2p-projekt.de	i2p-projekt.de

Table 2: Summary of censored countries, filtered I2P services, and blocking techniques detected.