Regional Variation in Chinese Internet Filtering

Joss Wright
Oxford Internet Institute,
University of Oxford
joss.wright@oii.ox.ac.uk

September 11, 2012

Abstract

Internet filtering in China is a pervasive and well-reported phenomenon and, as arguably the most extensive filtering regime in the world today, has been studied by a number of authors. Existing studies, however, have considered both the filtering infrastructure and the nation itself as largely homogeneous in this respect. In order to gain a deeper understanding of Chinese internet filtering, its practical effects and its social implications, it is crucial to understand in detail the extent to which filtering varies across China, and amongst its hundreds of millions of internet users.

This work investigates regional variation in filtering across China through direct access to internet services distributed across the country. This is achieved through use of the Domain Name Service, or DNS, which provides a mapping between human-readable names and machine-routable IP addresses on the internet, and which is thus a critical component of internet-based communications. Due to the key role that this service plays, its manipulation is a common mechanism used by states and institutions to hamper access to internet services that have been deemed undesirable.

Through access to a range of publicly available DNS servers located across China, obtained from the Asia-Pacific Network Information Centre (APNIC), we query data concerning known blocked websites. The results of these queries are compared against canonical results from unfiltered connections, allowing the detection of any tampering or blocking. By combining these results with the geographical location of each server, the nature of DNS-based filtering experienced in various parts of China can be analysed and mapped.

These experiments demonstrate that filtering varies widely across China, and occurs in several forms. Queries concerning blocked websites may result in valid responses, in faked responses that redirect to other servers, or in no response at all. We observe that individual servers do not typically respond in the same way for all blocked requests; nor is there a discernable overall geographic pattern to the nature or extent of filtering despite significant variation.

Our results support the hypothesis that, despite typically being considered a monolithic entity, the Golden Shield is better understood as a decentralised and semi-privatised operation in which low-level filtering decisions are left to local authorities and organisations. As such, the filtering experienced by a given citizen may vary wildly in the blocking technique employed, the ease by which the block can be bypassed, the level of collateral blocking that occurs, and the specific sites blocked at a given time.

This article provides a first step in understanding how filtering affects populations at a fine-grained level, and moves toward a more subtle understanding of internet filtering than those based on the broad criterion of nationality. The techniques employed in this work, while here applied to geographic criteria, provide an approach by which filtering can be analysed according to a range of social, economic and political factors in order to more fully understand the role that internet filtering plays in China, and around the world.
1 Introduction

Many nations around the globe participate in some form of internet filtering ([Deibert et al. 2008](https://www.ipe.org.au/)). Whilst filtering and censorship can, to an extent, be open and transparent, their nature tends towards secrecy. In order to understand the extent and nature of filtering around the world, we desire the ability to experience directly the limitations imposed on these internet connections.

National-level filtering, however, is simply the crudest form of such mapping. Whilst many states have national filtering policies, there is some evidence that the specific implementation of these may vary from region to region, from ISP to ISP and even from computer to computer. In order to fully understand filtering and its role in the globally networked world, it is extremely useful to explore connectivity at a more geographically and organisationally fine-grained level.

To this end, it is desirable to experience the Internet as viewed by a computer in a location of interest. There are a number of existing services specifically designed to allow this: virtual private network, or VPN, software and other proxy services allow remote computers to route their connections through a given remote network, and the well-known Tor ([Dingledine et al. 2004](https://www.torproject.org/)) anonymising network provides a similar service specifically aimed at bypassing national-level filtering.

For the purposes of wide-scale research, however, many of these services are relatively rare and require explicit access. Further, many of these services are employed directly to avoid filtering and thus to allow filtered users to access unfiltered connections. Clearly, such a service is less likely to exist on heavily filtered connections. In deliberately investigating filtered connections, it may be necessary also to explore other forms of information.

2 Motivation

There are a number of technical approaches to internet filtering employed around the world, varying in their severity and extent. The most well-known filtering regime is almost certainly China's Golden Shield Project (金盾工程 jīndùn gōngchéng) or 'Great Firewall', which represents arguably the largest and most technologically advanced filtering mechanism in use today at the national level.

Despite the technological sophistication of the Chinese national firewall, it is subject to a number of limitations. With a total population of roughly 1.3 billion and an internet population estimated at 5.13 million in 2011 ([CNNIC](https://www.cnnic.gov.cn/)) the number of Chinese internet users is comparable to the entire population of the European Union. At such a scale economies must be made in the mechanisms of filtering in order to limit the required computational and human resources to a manageable level. An excellent study of some of the major techniques employed by the underlying the Chinese national firewall was presented by [Clayton et al. 2006](https://www.ipe.org.au/).

Many other countries, however, perform internet filtering with significantly lower resources and technical investment. Technologies range from crude blocking of large portions of the internet, to sophisticated and subtle blocking of specific content. A global view of internet filtering has been comprehensively presented in [Deibert et al. 2008](https://www.ipe.org.au/). This work is notable not just for its scope, but for its focus on the sociological as well as technical aspects of filtering, covering the nature of filtered topics and the levels of state transparency in the filtering process.

At a national level, however, filtering beyond crude mechanisms is often considered infeasible due not only to computational, but also to the organisational requirements of such systems; even if sufficient technological resources are available, the dynamic nature of the internet imposes a significant administrative burden in maintaining up-to-date filtering rules.

In solving this second problem states may choose to provide broader filtering guidelines to be implemented by local authorities or individual service providers, resulting in potential differences between the filtering experienced between users in different geographical locations or those using different providers. It is also possible, and has been observed in a number of cases, that a state may deliberately choose to restrict internet services to a greater or lesser extent in certain locations as a result of unrest or disaster.

To understand the technologies employed by states in filtering the internet, and the decisions behind this filtering, we therefore see great interest in studying the extent and nature of filtering at a regional and organisational, rather than national, level. We believe that this will provide a much more sophisticated picture of filtering around the globe, and provide a valuable source of information for internet researchers.
3 Filtering Technologies

The development of the internet was neither carefully planned, nor accurately predicted. It has expanded through the accretion of protocols, services and applications that have been extended and improved far beyond their original purpose. As such, many of the protocols provide opportunities both for filtering technologies, and for attempts to bypass or study those technologies.

There are a number of methods applied to filter internet connections at a national level. These have been usefully categorised by Murdoch & Anderson (2008) as follows:

- **TCP/IP Header Filtering**: IP, the Internet Protocol, is the fundamental protocol by which traffic passes across the internet, encoded in IP packets. Filtering may occur via inspection of the header of an IP packet, which details the numerical address of the packet's destination. Packets may therefore be filtered according to lists of banned destination IP addresses. This method is simple and effective, but difficult to maintain due to the potential for services to change, or to have multiple, IP addresses. This approach may also incur significant collateral damage in the case of services that share IP addresses, causing multiple innocent services to be blocked along with the desired target.

- **TCP/IP Content Filtering**: Rather than inspecting the header, a filter may search the content of traffic for banned terms. This is a far more flexible approach to filtering, allowing packets to be blocked only if the include banned keywords or the traffic patterns of particular applications. This approach is also known as deep packet inspection, and is known to be employed to some extent by the Chinese national firewall. Deep packet inspection can be partially defeated by using encrypted connections, however filters may choose simply to block all encrypted connections in response, or to block traffic according to identifying traffic signatures that can occur even in encrypted protocols. The most significant limitation of this approach is that inspection of traffic content comes at a significant computational cost.

- **DNS Tampering**: The DNS protocol maps human-readable names to IP addresses on the internet, and is thus critical for most user-focused services such as the web. By altering DNS responses, returning either empty or false results, a filter can simply and cheaply block or redirect requests. This mechanism is simple to employ and maintain, but limits filters to entire websites, and can be relatively easy to bypass for technical users. This approach is typically employed as a first approach to web-based filtering, due to its low resource requirements and in spite of its ease of bypass, however it has been noted that states typically graduate to more sophisticated filtering techniques over time (Deibert et al. 2008).

- **HTTP Proxy Filtering**: A more sophisticated approach is to pass all internet traffic through an intermediary proxy server that fetches and, typically, caches information for users. This is a common internet service that can be used to speed up internet connections and reduce traffic. A suitably enabled proxy can, however, employ sophisticated filtering on certain destinations, whilst leaving other connections alone. This approach can, by ignoring the majority of traffic, be efficient on a national scale while still allowing for detailed filtering similar to TCP/IP content filtering.

- **Other Approaches**: A variety of other means can be taken to regulate content on the internet. States can request that websites are removed from the internet, either by taking down their servers or by removing their names from the global DNS records. A state may also choose not to block a connection entirely, but to slow any connection to that site to unusable levels. At a less technical level, legal and social constraints can be imposed to may accessing certain services illegal or socially unacceptable.

It has been noted, in Deibert et al. (2008) that many states begin by employing IP header filtering before moving on to more sophisticated methods as citizens protest the limiting of their connections. In the case of sophisticated national-level connections it is likely that a combination of these methods will be employed in order to meet the various constraints of large-scale filtering.

4 Mapping Filtering

A number of projects exist that provide insight into internet censorship around the world, both from the perspective of discovering filtered sites and keywords, and from the more concern of bypassing filtering. The most thorough study of global internet filtering is from Deibert et al. (2008), who present an in-depth global
study of tools and techniques of filtering. The related Herdict project (The Herdict Project n.d.) allows users to report apparently blocked websites, via a browser plugin, to build up a global map of filtered sites. The Alkasir project (Al-Saqaf n.d.) combines user-based reporting of blocked content with an anti-censorship tool that attempts to penetrate such filtering.

In bypassing internet filtering, perhaps the most well-known technology internationally is the Tor project (Dingledine et al. 2004), which allows users to reroute their connections through a global network of volunteer-run anonymising proxy servers. This network, originally designed to preserve the connection-level privacy of users, was found to be an excellent tool for bypassing national filtering and now invests significant resources in supporting this use. Similar tools include Psiphon (Psiphon Inc. n.d.) as well as numerous Virtual Private Network (VPN) servers that allow users to evade national filters. All of these services work in a similar manner: by rerouting a connection through a server located in a different country, the user experiences the internet as if their connection originated in that country. Thus, a user from Saudi Arabia is able to route their connection through a US computer and bypass all filtering imposed by their state or organization, at the cost of some slowing of their connection and gaining any filtering or surveillance, if any, imposed by the US or the provider of the proxy.

From these examples, we can observe two major possibilities for studying internet filtering. The first is to ask users in a given country to report their experience, as exemplified by the Herdict project; the second is to make use of an available service, such as a Tor node, in that country to experience the filtering directly. Both of these approaches have limitations that we explore in detail below.

Fundamentally, both of the aforementioned approaches suffer from a lack of availability that we see no easy way to avoid. In requesting users to directly report their experiences, Herdict relies on reaching interested and informed users. Tor relies on technically knowledgeable users to set up relays that require both significant resources and a willingness to face potentially serious legal issues (The Electronic Frontier Foundation n.d.). In particular, at time of writing the Tor network does not report any publicly available servers in China.

The advantage of using a system such as Tor, Psiphon or VPN services is that they allow a researcher directly to control the flow of traffic. Sites of interest and even specific patterns of traffic can be directly sent and examined. This allows for a much more detailed examination of the technical measures employed on a given network. The approach taken by Herdict, however, cannot currently reproduce this level of sophistication. In the absence of a large network of experienced and technically capable users, user-level reporting only provides that a site appears to be unavailable, without reference to the conditions that cause the unavailability.

In order to achieve the fine-grained mapping of filtering that we desire, there are two major points of interest beyond those commonly considered by the most well-known current mapping projects. The first of these is the precise geographical location of a particular computer. The ability to determine the originating country of an IP address is relatively well known, and location to the level of an individual city can be achieved with some accuracy. Recent results from Wang et al. (2011) have proposed mechanisms that achieve a median accuracy of 690 metres, albeit within the US. This simple extension, we propose, would provide a valuable source of data on the applications of filtering. In many cases it is also possible to determine which organisation has been allocated any particular IP address, to the level of an ISP or major company. Both of these pieces of information can be used to build up a much more detailed view of filtering.

The second point of interest is to study, in detail, the technical nature of the filtering that is imposed on a given connection in a given location. While work has been conducted into specific methods, as in the work of Clayton et al. (2006) relating to the Chinese national filter, most large-scale projects appear to be focused more on the existence of filtering rather than the details of its implementation.

4.1 Extending Reporting Approaches

The approach taken by the Herdict project, which relies on volunteer participation to gather data, can be highly effective if sufficient volunteers can be found. Herdict currently provides a webpage that attempts to direct a user’s browser to load a random potentially-blocked site, and to report their experience. The

---

1 Specifically, there are no announced exit nodes, which would be the most feasible way to examine network filtering, reported as located on the Chinese mainland.

2 The Herdict project does allow a user to express their opinion as to the cause of the blocking, but in the absence of direct experimentation this data has significant limitations.
The project also makes available a web browser plugin that allows users to report sites that appear blocked. By focusing on the web browser environment, Herdict greatly reduce the effort required for user participation. The importance of this approach to usability, and the trust implicitly gained through the familiarity of the web browser, should not be overlooked.

This volunteer approach could naturally be extended to the use of more sophisticated tools to detect the presence of filtering automatically and, where possible, test the mechanisms employed. The detection of DNS filtering, IP blocking and even deep packet inspection is often simple enough in itself, particularly when the results of requests can be compared against reference requests made in other countries. It is, however, much more difficult to discover specifics of filtering mechanisms without direct, interactive access to the filtered network connection.

5 Ethics and Legality

While many technical approaches, and challenges, exist for mapping global filtering, there are a number of serious legal and ethical issues to be faced with performing this research.

Deliberate misuse of a network service, for the purposes of detecting internet filtering, may be illegal in many jurisdictions; such misuse without a user’s consent may well be unethical. Even when using openly available and general purpose services, however, there are serious considerations when attempting to access blocked content via a third party.

In many situations, a user is unlikely to face repercussions for being seen to be attempting to access blocked content. The scale of internet use, even in smaller countries with low internet penetration rates, is simply too high for there to be serious policing of users who request filtered content. It is likely that, in the vast majority of cases, such attempts may not be logged at all. However, users in specific contexts may be put at risk.

The legality of attempting to access filtered content is also a concern. Many nations have somewhat loosely defined computer crime laws, and often prefer to prosecute crimes involving computers under existing legislation rather than through creation of new laws (Lessig 2006). The legal status of attempting to access blocked content, however, and of attempting to bypass such blocks is not something a researcher can afford to ignore.

From the point of view of a researcher, these concerns are exacerbated by two factors: the concentrated attempts to access filtered content that is caused by a detection tool, and the wide variety of laws and social conventions that are encompassed by researching a global phenomenon such as censorship.

By their nature, the filtering detection mechanisms that we have discussed, and any that we can feasibly imagine, detect filtering through attempts to access filtered content: websites or IP addresses that are known, or are believed or likely, to be banned. As we have stated above, it would be largely impractical for a state to take note of every blocking action taken by their filter; it is possible, however, that sufficiently high-volume requests for banned content may be considered worthy of further action. A user innocently aiding a researcher in mapping censorship, resulting in their computer suddenly attempting to connect to all forms of banned content, may find themselves under highly unwelcome scrutiny.

It is also of great concern that a researcher not cause a user to unwittingly break the law with respect to the content that they direct a user to access. With the wide global variance in law, great care must be taken that a censorship tool not attempt to access content that was directly illegal. Pornography, particularly with respect to those under the local age of legal consent, lèse majesté and insults to religion are all sensitive issues that vary widely between cultures.

Volunteers that participate in research of this nature by running a filtering detection tool must do so having been fully informed as to the nature of the tool and the potential risks involved. From this perspective there is a significant added burden on the researcher to state to the participant, who may well not have any significant level of technical expertise, what the tool will do and what particular risks they run.

In the case of relay services, such as Tor or Psiphon, consideration must be given to the safety and security of the user operating the service. Due to their nature these services are frequently abused, and operators of such services must be prepared to defend their operation of the service. The Tor Project, in particular, invests significant efforts in education both for operators and for users. This does not, however, reduce the burden on a researcher taking advantage of such a service to ensure that they do not harm or endanger the operator.
through their actions.

6 Experiments

To conduct a direct investigation of regional variations in censorship across China, access through the DNS service was selected as the most appropriate mechanism. DNS provides a number of attractive features for both technical and for legal and ethical reasons.

At a technical level, due to their crucial role in resolving names to IP addresses, DNS servers are both common and widespread, providing the desired level of coverage across the country to an extent that is difficult to match with other approaches. DNS servers are also often openly accessible, meaning that there is no technical restriction in making requests to these remote systems.

DNS servers are also attractive as they are typically run either by internet service providers for the benefit of their customers, or by large organizations that run their own networks. The result of this is that the results returned by a given DNS server typically reflect the view of the internet, at the level of DNS, of a reasonably large class of users.

From a legal and ethical point of view, DNS servers have the advantage of functioning, at an extremely simple level, as a simple database of mappings between domain names and IP address. As such, requesting information regarding a given mapping between a domain and an address does not cause any direct access to potentially sensitive resources on behalf of a third party, as would be the case for the proxy services mentioned above.

To obtain a useful sample for investigating DNS censorship across China, a list of DNS servers was retrieved from the Asia Pacific Network Information Centre (APNIC), the Regional Internet Registry responsible for allocating IP addresses and Autonomous System (AS) numbers across the Asia Pacific region. This organization maintains a database, known as a WHOIS database, that stores information regarding registered domain names in their region, including the authoritative DNS servers for each domain. From the WHOIS records, a list of 278 DNS servers apparently located in China, according to our geolocation service, was retrieved of which 187 were found to be available and responsive to remote queries.

In order to incorporate geographical information in our results we make use of the freely-available MaxMind GeoIP database ([MaxMind Inc. n.d.]) to resolve IP addresses to the city level with a tolerable level of accuracy. This thus allows us to identify the location of almost all DNS servers in our test set. It is worth noting, as we shall discuss later, that this does not represent the location of the users of that service; these users make DNS requests from their home network connection, and could potentially be located in almost any geographical location, but will in practice almost certainly be within China.

We made use of the Herdict project ([The Herdict Project n.d.]), operated by the Harvard Berkman Centre, to retrieve a list of domain names that had been reported as blocked in China. The Herdict project makes use of crowdsourced reporting to maintain a list of websites for which users have experienced some form of filtering or censorship, sorted according to country, and thus provides a useful source of data for potentially blocked domain names.

The Herdict project lists the most frequently reported blocked websites for each country, each list comprising the top 80 reported domains. In addition to this, we included five popular Chinese websites that, presumably, would not be blocked in mainland China. A full list of tested domains is given in Appendix A.

To learn the scope and scale of blocking, each potentially-blocked domain name in the list retrieved from Herdict was requested from each DNS server retrieved from the APNIC WHOIS database. These results were recorded and analysed according to the nature of the DNS response received in each case.

In order to determine whether the results returned were genuine, an equivalent query was conducted on a self-managed DNS server located in a country that does not perform extensive internet filtering. The results

---

3 Strictly speaking, DNS servers return the IP for a particular hostname, many of which may fall under a given domain. For the purposes of this article, the two may be considered functionally equivalent as we will not request multiple hosts for a single domain.

4 For completeness, it should be mentioned that DNS servers function in a hierarchy, and may request information for unknown domain names from more authoritative servers. This normal function of the service would not, however, implicate any third party, and would in fact be directly traceable to the computer used in our experiments.

5 In the case of the experiments detailed here, this was the United Kingdom. Whilst the United Kingdom certainly does engage in national-scale internet filtering, care was taken that such filtering would not affect the results of these experiments.
of the remote query were compared heuristically with the local result, any differences were noted.

In order to minimise genuine short-term network errors, the sequence of requests was repeated six times at one-hour intervals. The results from the different experimental sets were combined in such a way that timeouts, which could represent genuinely poor connectivity, were eliminated unless they were seen to be consistent across all result sets.

6.1 DNS Response Types

The categorization presented in §3 identifies four major filtering techniques, of which DNS poisoning is one. Manipulation of DNS can, however, take on a number of forms, of which some could represent either censorship or genuine errors. The most important behaviours of a DNS server, for the purposes of this article, are discussed here.

• **Invalid Server Errors**
  A DNS server, on receiving a given query, may respond with an indication that it is not, in fact, a DNS server. In this case, the requesting party will not receive a mapping from the requested name to an IP address, and thus cannot proceed with making a connection. Clearly, such a response could also indicate that the requested party was genuinely not, in fact, a DNS server.

• **Timeout Errors**
  A simpler behaviour, and one that is harder to categorize unambiguously as censorship, is for a DNS server to accept requests, but not to respond in any way for blocked domains. Eventually, the requesting party will exceed a given time threshold and abandon the query. This again prevents the client from learning the IP address of the requested host, and could be ascribed to a genuine network error. A secondary effect of such an approach is that the requesting party does not receive an immediate response, which may cause internet requests to blocked sites to pause until the timeout threshold is reached.

• **Unknown Domain Errors**
  The simplest form of direct DNS censorship is for the DNS server to deny the existence of the requested website, causing the requesting party to receive an error. For known existing domains, this response is easily identifiable as malicious behaviour on the part of the server.

• **Misleading Results**
  A more subtle approach to censorship is for requests for blocked websites to generate a valid DNS response, providing the client with an IP address for the requested hostname, but to provide false information in the form of an incorrect IP address.
  This approach has several potential implications, which will be discussed further below. One potential outcome of such an approach is that the requesting party may be directed to a host that logs all attempts to access banned websites, allowing for a level of surveillance or monitoring of such requests.

• **Genuine Results**
  The final possibility that we consider is that the DNS server returns the IP address that corresponds to the requested hostname. While this particular piece of information may be accurate censorship may, of course, occur through one of the other techniques discussed in §3.

7 Results

We discuss here the results of querying DNS servers across China for reportedly-banned domain name, discuss the general trends in the responses, and isolate a number of particularly unusual observed behaviours.

---

6Specifically, the first two dotted quads of the IP addresses returned by the remote and the local DNS server were compared. If these differed, the response was marked as incorrect. In order to accommodate internet services that use content distribution networks that employ a wider range of IP addresses, the results were manually examined to detect any such networks, which were in turn whitelisted. We accept that this automated approach does allow a small chance of introducing both false positives and false negatives with respect to the existence of misleading DNS results.
domain No Domain No Answer No Nameserver Timeout True IP False IP
twitter.com 0 1 12 6 3 165
www.backchina.com 0 0 13 7 5 162
www.youtube.com 0 0 14 7 6 160
www.ntdtv.com 0 0 23 7 0 157
www.open.com.hk 0 1 20 7 3 156
www.torproject.org 0 2 24 7 1 153
www.tibet.net 0 2 22 7 3 153
www.peacehall.com 0 1 20 7 6 153
www.facebook.com 0 1 26 7 0 153
www.6park.com 0 0 26 7 2 152

Figure 1: Ten most misdirected domains from experiments, showing DNS error result counts for each domain.

7.1 Broad Trends

Overall, experiments were conducted on 187 DNS servers across China, 178 of these servers answered at least one query with a valid, but not necessarily truthful, IP address. Of the responding servers, 79 answered at least one query with a response that appeared to be accurate, meaning that 99 servers returned only invalid results for the requested domains.

A small number of servers were clearly either misconfigured, or deliberately providing invalid results to our requests. Five servers consistently timed out on DNS requests, despite an allowance for an artificially long timeout period of 60 seconds. One server consistently produced an invalid nameserver error, despite apparently accepting DNS requests.

We discuss below the general trends observed in the overall result sets, before moving on to specific examples.

7.1.1 Widespread DNS Poisoning

Our experiments provide evidence of widespread manipulation of DNS results, occurring in all the forms discussed in the previous section. Interestingly, individual DNS servers do not, in general, display consistent blocking behaviour across all domains, but may instead return an incorrect IP address for one domain, claim that a second domain does not exist, and refuse to respond to requests for a third domain.

Figure 1 demonstrates the ten most widely misdirected domains observed in experiments. These domains were thus almost universally blocked across China. It should be noted that, in addition to an overwhelming majority of misleading results for each domain, the remaining servers were likely either to time out or to claim not to be a valid nameserver for this result.

Figure 2 lists the ten domains that are most often claimed not to exist by the tested DNS servers. As can be seen, claiming a domain to be non-existent is far less common than providing an inaccurate IP address result. It is worth noting that the domains listed in Figure 2 receive large numbers of timed-out requests, as well as both accurate and inaccurate IP responses.

These results suggest that approaches to DNS poisoning favour misdirection of domains over claims that the domain does not exist, and that allowing a request to timeout by not responding, as opposed to generating an error, is also common approach.

7.1.2 Timeout Responses

The prevalence of timeouts in our results could potentially be explained by filtering occurring not directly at the DNS servers, but instead at other points in the network.

The DNS protocol, unusually, makes use of an underlying internet transport protocol known as UDP, as opposed to the more common TCP protocol employed by the majority of internet services such as the world-wide web. This protocol has the advantage of higher speeds and lower transmission overheads, but
Domain | No Domain | No Answer | No Nameserver | Timeout | True IP | False IP \\
---|---|---|---|---|---|---
www.ahrchk.net | 4 | 17 | 64 | 40 | 60 | 2 \\
killerjo.net | 4 | 17 | 65 | 37 | 62 | 2 \\
www.x365x.com | 3 | 17 | 65 | 41 | 59 | 2 \\
www.websitepulse.com | 3 | 18 | 65 | 36 | 63 | 2 \\
www.voanews.com | 3 | 17 | 64 | 38 | 63 | 2 \\
www.tumblr.com | 3 | 17 | 64 | 38 | 37 | 28 \\
www.steves-digicams.com | 3 | 17 | 65 | 36 | 64 | 2 \\
www.scribd.com | 3 | 17 | 65 | 36 | 38 | 28 \\
www.pinyinannotator.com | 3 | 18 | 67 | 36 | 61 | 2 \\
www.newgrounds.com | 3 | 16 | 64 | 36 | 66 | 2 \\

Figure 2: Ten domains most often claimed non-existent.

does not provide guarantees that data will be delivered, nor does it allow for confirmation of message delivery. It is therefore the case that, if DNS requests for particular domains were blocked or dropped in the network, that it would be difficult to detect this fact; the result would be observed simply as a timeout.

Another alternative is that the DNS servers in question, upon receiving a request for a blocked domain, simply ignore the request. From the experiments detailed here, it is difficult to verify either of these claims. It seems likely, however, that filtering of DNS traffic in transit to block requests would be more complex and costly, and would result in a more homogeneous and extensive pattern of timeouts than were observed. As such, the argument for filtering at the server level, or some combination of both arguments, appears most likely.

7.1.3 Common Misleading IP Addresses

An examination of the results returned from the experiments show that, in the case that a DNS server returns an IP address that does not correspond to the requested domain, the returned IP address is drawn from a comparatively small pool of possible responses; misleading IP addresses are neither random nor returned on a per-server basis.

Our experiments made requests for 85 domains to 187 DNS servers, resulting in a total of 15,895 requests in total. Of these requests 6658 gave a response that pointed to an IP address, 2258 of which were judged by our analysis to be misleading. These 2258 misleading results each pointed to one of only 84 IP addresses, meaning that there is significant correlation between the misleading IP addresses returned by DNS servers across the country.

Two possible explanations exist for this result, assuming that our analysis of misleading IP addresses is correct. The first is that a centralized list exists that provides specific DNS poisoning instructions, including IP address, for DNS server operators. The second possibility is that the DNS responses observed in our experiments, being conducted outside of China and therefore travelling across the nation’s border routers that are known to engage in substantial filtering, were manipulated in transit. Investigation of these two possibilities is a subject for future work.

7.2 Domain Statistics

We discuss here a number of results that exemplify observed filtering behaviour according to the particular domains queried in these experiments.

7.2.1 Poisoning of Uncensored Domains

In addition to the list of 80 domains obtained from the Herdict project, our experiments incorporated domain names for five popular Chinese internet services with the intention that these would be unfiltered. Surprisingly, in several cases our results appeared to show misleading results for a number of these domains.
<table>
<thead>
<tr>
<th>Server</th>
<th>Location</th>
<th>Remote Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>202.95.0.10</td>
<td>China, Beijing</td>
<td>renren.com. 900 IN A 123.125.38.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>renren.com. 900 IN A 123.125.38.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>renren.com. 900 IN A 123.125.38.239</td>
</tr>
<tr>
<td></td>
<td></td>
<td>renren.com. 900 IN A 123.125.38.240</td>
</tr>
<tr>
<td></td>
<td></td>
<td>renren.com. 900 IN A 123.125.38.241</td>
</tr>
<tr>
<td>121.101.208.41</td>
<td>China, Chaoyang</td>
<td>renren.com. 900 IN A 123.125.38.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>renren.com. 900 IN A 123.125.38.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>renren.com. 900 IN A 123.125.38.239</td>
</tr>
<tr>
<td></td>
<td></td>
<td>renren.com. 900 IN A 123.125.38.240</td>
</tr>
<tr>
<td></td>
<td></td>
<td>renren.com. 900 IN A 123.125.38.241</td>
</tr>
</tbody>
</table>

Figure 3: Inaccurate results for renren.com. Distinct servers show identical incorrect results.

We have not determined whether this represents misconfiguration of DNS servers, deliberately invalid results returned due to our request originating outside of China, or some other cause.

An illustrative example is that of renren.com, a popular Chinese social network. In at least two cases, invalid IP addresses were returned for this service, as shown in Figure 3. In this example, the two servers are located in different cities, and are apparently operated by separate companies; both are certainly both logically and physically distinct. Despite this, both servers return the same list of IP addresses, none of which appear to belong to servers of renren.com.

On directly querying the addresses in question, a number of them appear to be running an unconfigured webserver. It is not known what, if any, the significance of these addresses may be.

7.2.2 Purposeful Misdirection of torproject.org

The Tor Project produce a number of tools that aim to provide anonymous and untraceable internet communications, as well as to bypass censorship. As such, both the tool and the project website are commonly blocked in countries with extensive internet censorship.

On querying servers for the Tor Project's website, eighteen apparently unrelated servers instead returned results for an entirely separate domain: tonycastro.com. This domain is not in any discernible way linked to the Tor Project, except in that both domains begin with the letters 'to', and are ten characters in total, suggesting that some form of substitution had occurred in the DNS records. While this could be a pure coincidence, the number of results from disparate servers all pointing to the same domain strongly imply some broader connection.

The Tor Project appears to be the only domain on the tested list that suffers from this, particularly curious, form of filtering.

7.3 Server Statistics

We examine here a number of statistics concerning the behaviour of servers across the range of queried domains.

7.3.1 Exemplar Misleading Results

The majority of servers queried in our experiments returned a mix of result types, with varying degrees of misleading results. A small number of DNS servers, however, demonstrated an unusually extreme range of negative responses, and are thus demonstrative examples of the invalid responses given.

IP Address: 113.11.192.25

This server is apparently located in Beijing. Over the course of 85 domain name requests, this server responded with a 'no answer' reply 68 times. This included the five valid services, including Baidu and
<table>
<thead>
<tr>
<th>Server</th>
<th>Location</th>
<th>Domain of Returned IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>58.20.127.238</td>
<td>China, Changsha</td>
<td>tonycastro.com</td>
</tr>
<tr>
<td>61.135.238.2</td>
<td>China, Beijing</td>
<td>tonycastro.net</td>
</tr>
<tr>
<td>122.102.0.10</td>
<td>China, Chaoyang</td>
<td>tonycastro.com</td>
</tr>
<tr>
<td>159.226.161.126</td>
<td>China, Beijing</td>
<td>tonycastro.com</td>
</tr>
<tr>
<td>159.226.8.6</td>
<td>China, Beijing</td>
<td>tonycastro.net</td>
</tr>
<tr>
<td>159.226.8.6</td>
<td>China, Beijing</td>
<td>tonycastro.org.ez-site.net</td>
</tr>
<tr>
<td>202.101.98.54</td>
<td>(Unknown Location)</td>
<td>tonycastro.org.ez-site.net</td>
</tr>
<tr>
<td>202.102.134.69</td>
<td>China, Jinan</td>
<td>tonycastro.net</td>
</tr>
<tr>
<td>202.103.64.139</td>
<td>China, Changsha</td>
<td>tonycastro.net</td>
</tr>
<tr>
<td>202.103.96.66</td>
<td>China, Changsha</td>
<td>tonycastro.net</td>
</tr>
<tr>
<td>202.38.128.10</td>
<td>China, Beijing</td>
<td>tonycastro.net</td>
</tr>
<tr>
<td>202.38.64.56</td>
<td>China, Hefei</td>
<td>tonycastro.org.ez-site.net</td>
</tr>
<tr>
<td>202.95.0.10</td>
<td>China, Beijing</td>
<td>tonycastro.com</td>
</tr>
<tr>
<td>202.99.224.200</td>
<td>China, Baotou</td>
<td>tonycastro.org.ez-site.net</td>
</tr>
<tr>
<td>203.207.119.8</td>
<td>China, Beijing</td>
<td>tonycastro.com</td>
</tr>
<tr>
<td>210.45.224.1</td>
<td>China, Hefei</td>
<td>tonycastro.org.ez-site.net</td>
</tr>
<tr>
<td>220.250.64.18</td>
<td>China, Beijing</td>
<td>tonycastro.org.ez-site.net</td>
</tr>
<tr>
<td>221.5.203.99</td>
<td>China, Chongqing</td>
<td>tonycastro.org.ez-site.net</td>
</tr>
<tr>
<td>222.66.238.4</td>
<td>China, Shanghai</td>
<td>tonycastro.com</td>
</tr>
</tbody>
</table>

Figure 4: torproject.org requests resolving to alternative domain.

RenRen in our test set, and may indicate discrimination against our requests due to being located outside of China.

A further 13 requests resulted in the return of a valid IP address. On examination, all of these IP addresses were found to be unassociated with the requested domain. The list of domains and associated IP addresses can be found in Figure 5.

Of interest, rather that simply the fact that a misleading IP address was returned, is the nature of the IP addresses in question. There was no discernable pattern in these results; they point to seemingly-random hosts corresponding to domains and organisations that do not appear to have any connection with each other or with the originally requested domain. It is notable, however, that certain of the blocked domains point to the same IP addresses, even though those IP addresses are not related to the domain in question. As can be seen from Figure 5, both YouTube and Facebook redirect to the same IP address, as do peacehall.com and wujie.net, and backchina.com, boxun.com and open.com.hk.

The remaining four domains requested from this server resulted in a claim that no such domain existed.

**IP Address: 202.99.224.203**

This server is apparently located in Baotou. Of 85 domains, the majority of results were to claim that the server was not valid for returning DNS requests. In total, requests for 14 domains resulted in one or more IP addresses being reported, none of which led to the appropriate servers. This behaviour, to appear invalid for some domains and to return fake results for others, was particularly strange.

It could once more be observed that, although invalid IP addresses were returned, these were not purely random but instead were consistent for each domain, and were drawn from a small pool of IP addresses that were used multiple times for different domains.

### 7.3.2 Localhost Redirection

An interesting choice of address to return when providing inaccurate IP addresses is to point the request back to the computer from which it originated. This can be achieved through use of the special ‘reserved’ IP address 127.0.0.1, which also has the DNS designation of ‘localhost’.
### Domain and Returned IP

<table>
<thead>
<tr>
<th>Domain</th>
<th>Returned IP</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.hotspotshield.com">www.hotspotshield.com</a></td>
<td>8.7.198.45</td>
</tr>
<tr>
<td><a href="http://www.tibet.net">www.tibet.net</a></td>
<td>159.106.121.75</td>
</tr>
<tr>
<td><a href="http://www.boxun.com">www.boxun.com</a></td>
<td>46.82.174.68</td>
</tr>
<tr>
<td>wezhiyong.org</td>
<td>8.7.198.45</td>
</tr>
<tr>
<td><a href="http://www.backchina.com">www.backchina.com</a></td>
<td>46.82.174.68</td>
</tr>
<tr>
<td><a href="http://www.ntdrv.com">www.ntdrv.com</a></td>
<td>8.7.198.45</td>
</tr>
<tr>
<td><a href="http://www.peacehall.com">www.peacehall.com</a></td>
<td>59.24.3.173</td>
</tr>
<tr>
<td><a href="http://www.youtube.com">www.youtube.com</a></td>
<td>203.98.7.65</td>
</tr>
<tr>
<td><a href="http://www.facebook.com">www.facebook.com</a></td>
<td>203.98.7.65</td>
</tr>
<tr>
<td>twitter.com</td>
<td>159.106.121.75</td>
</tr>
<tr>
<td><a href="http://www.wujie.net">www.wujie.net</a></td>
<td>59.24.3.173</td>
</tr>
<tr>
<td><a href="http://www.6park.com">www.6park.com</a></td>
<td>159.106.121.75</td>
</tr>
<tr>
<td><a href="http://www.open.com.hk">www.open.com.hk</a></td>
<td>46.82.174.68</td>
</tr>
</tbody>
</table>

**Figure 5:** Misleading IP addresses from a Beijing-based DNS server.

Local redirection has the advantage of not requiring a genuine IP address to be selected from the internet, which can lead to undesirable behaviour. It also minimises traffic passing over the internet, as any further requests made to this connection remain on the user’s computer without travelling over the general internet.

Despite this, the use of redirection to the localhost was not particularly widespread amongst the queried servers. Of the 187 servers queried only six servers returned results pointing to the localhost, of which four consistently returned the localhost for any DNS query. This could represent either a misconfigured DNS server, or a blanket policy for unauthorized or non-Chinese requests.

Two servers, however, with addresses 202.99.224.200 and 202.99.224.223 returned 127.0.0.1 for the majority of requests, but also resulted in an invalid nameserver error for seven domains. In 13 cases, however, an IP response was given that, again, appears random, resolving to Azerbaijani, Irish, US, Italian, New Zealand owned hosts.

### 8 Geographical Distribution

Figure 6 presents an overview of the variations in filtering observed across the various cities covered by our experiments. Darker grey markers represent a greater percentage of misleading DNS responses compared to accurate responses. As results were obtained for potentially many servers within a given city, the median average percentage of all results observed for all servers in the city is represented. To indicated cities with a larger number of DNS servers, markers are scaled according to the number of servers tested, ranging from a single server in cities such as Dongguang and Harbin, to 72 servers in Beijing.

Whilst we do not observe any overall pattern to the filtering experienced in different cities, there is clear heterogeneity across the country. This supports the view that high-level controls over filtering are relatively loose in terms of implementation of filtering, with the technical details of blocking being decided at the local rather than regional or national level.

### 9 Experimental Limitations

There are a number of limitations to the experimental methodology that we employed in this work, which we will detail briefly here.

The first and most obvious is that the experiments relied on a restricted list of DNS servers obtained from the APNIC WHOIS database. Whilst the set of servers used provided a reasonable coverage of China geographically, although with a notable bias towards the East of the country, there was a great disparity between the number of servers observed in each city. This figure ranged from 72 servers in Beijing, to only
Figure 6: DNS queries across China showing median percentage of misleading results for queried domains, with darker points representing a higher percentage of misleading results. Circle size represents the relative number of servers queried in each city.
one server in several of the smaller cities. While this will, to some extent, reflect the realities of DNS server placement in China, it appears insufficient for a genuine analysis of the relative experience of internet users.

A more fundamental limitation is that DNS servers are not necessarily, or usually, located in the same geographical area as a user. A DNS server is typically operated and managed by an ISP and made available to its users automatically. It is therefore likely that a given ISP's customers, who may be widely dispersed, all use the same DNS server. As such, the results presented here arguably represent organizational variation, rather than geographical.

Ongoing research is being conducted into means to extend the approach presented here to allow direct remote IP scanning to detect reachability between two remote systems. This approach, by revealing actual traffic flows rather than the simple routing information returned by DNS queries, allows a much deeper and effective analysis of filtering behaviour. In particular, recently discovered forms of remote scanning (Ensafi et al. 2010) provide a promising avenue for this work, and would largely eliminate the previously mentioned limitations.

Further, the results in this article represent a snapshot taken in mid-2012, and as such cannot reflect the changing patterns of censorship. Given the automated nature of these tests, however, and the relatively short time required to conduct them, the gathering of time-series data is a relatively small step, and has the potential to reveal useful patterns of censorship over time.

The final major limitation to this work is that it provides a purely technical view of one form of filtering occurring in China. These results provide a window into the limitations imposed on users' internet connections, but can provide little data with respect to the effects of censorship on users' browsing behaviour, social attitudes to various forms of content, choice of forums, modes and means of communication, and access to news sources. As such, the experiments detailed here provide only a limited first step in understanding the wider phenomenon of internet censorship.

10 Conclusions

We have proposed that it is, in general, false to consider internet filtering as an homogeneous phenomenon across a country, and that the practicalities of implementing a filtering regime are likely to result in geographical and organisational differentiation between the filtering experienced by users.

We believe that the study of these differences are of great interest in understanding both the technologies and the motivations behind filtering, and have proposed a number of mechanisms that could be employed to gain this understanding.

Despite the existence of a number of technological and social avenues to aid in this research, we see a number of serious legal and ethical concerns that must be thoroughly considered in order to undertake broad-scale research of this nature. Beyond the more obvious pitfalls of misusing third-party services in an attempt to conduct this research, there are more subtle issues. The necessity of attempting to access blocked content, and the legality and ethics of performing this via a third-party volunteer or service operator are all worthy of serious discussion by researchers in this field.

In response to the technical and ethical challenges of censorship research, we have conducted a nation-wide remote survey of the apparent filtering experienced by Chinese internet users, with specific reference to blocking attempts that occur through the Domain Name Service (DNS). These experiments have revealed widespread poisoning of DNS results, including invalid server responses, valid domains claimed to be non-existent, and the return of IP addresses that do not correspond to the requested domain.

Our analysis of these results has revealed a number of trends in this filtering, most notably the prevalence of misleading responses for domains over claims that domains do not exist. Further, although the extent of filtering varies geographically, we have identified correlations in the misleading IP addresses returned in response to requests for blocked domains by different servers, implying some level of top-down involvement in the behaviour of servers.

Despite the concerns raised in ethically researching internet censorship, and the technical hurdles to gaining a detailed picture of global internet filtering, we consider that research into this subject presents a number of interesting problems, and can provide insight into the development of the internet and its ongoing social and political role both the national and international level.
A  Tested Domain Names

The following domain names were tested against the list of available DNS servers:

A.1  Reported Blocked

These domains were retrieved from the Herdict Project, and have thus been reported multiple times as blocked within China.


A.2  Common Services

These domains represent popular Chinese services that were anticipated not to be blocked within China.

baidu.com - qq.com - caixin.com - renren.com - chinaview.cn

References


**URL:** [http://www.worldcat.org/isbn/0262541963](http://www.worldcat.org/isbn/0262541963)


