To appear in *Proceedings of the 3rd USENIX Workshop on Free and Open Communications on the Internet*, August 2013.

Internet Censorship in Iran: A First Look

Simurgh Aryan *
Aryan Censorship Project
aryan.censorship.project@gmail.com

Homa Aryan *
Aryan Censorship Project
aryan.censorship.project@gmail.com

J. Alex Halderman
University of Michigan
jhalderm@umich.edu

Abstract

The Iranian government operates one of the largest and most sophisticated Internet censorship regimes in the world, but the mechanisms it employs have received little research attention, primarily due to lack of access to network connections within the country and personal risks to Iranian citizens who take part. In this paper, we examine the status of Internet censorship in Iran based on network measurements conducted from a major Iranian ISP during the lead up to the June 2013 presidential election. We measure the scope of the censorship by probing Alexa's top 500 websites in 18 different categories. We investigate the technical mechanisms used for HTTP Host–based blocking, keyword filtering, DNS hijacking, and protocol-based throttling. Finally, we map the network topology of the censorship infrastructure and find evidence that it relies heavily on centralized equipment, a property that might be fruitfully exploited by next generation approaches to censorship circumvention.

1 Introduction

Iran is known as one of the leading suppressors of Internet freedom. Reporters Without Borders ranks Iran as one of the "twelve enemies of the Internet" [33], and Freedom House has dubbed it the "least free" country in terms of Internet freedom [23]. Iran's Internet censorship goes beyond simply blocking access to particular websites and services. Some conservative voices have called for the creation of a fully separate "Halal Internet," which would contain only content allowed by their strict interpretation of Islamic law [35]. Although the government's stated policies fall short of this extreme view [1], it recently created a Cyber Police unit, FATA [19], which monitors Iranians' online activities and prosecutes dissidents [10]. High ranking officials have actively encouraged adoption of domestic sites for applications like blogging, email, and social media [31, 39], while censorship and connection throttling discourage use of similar services hosted abroad, which are more difficult to police.

While these developments have been widely reported, little research has been conducted on the technology and network topology behind Iran's Internet censorship regime. Probing the network from within the country is dangerous, due to a climate of heavy government control and personal risks to Iranian citizens who take part. Despite these risks, this study seeks to narrow the gaps in our knowledge by providing a firsthand view of how Internet access is being restricted in Iran.

To conduct our study, we established a small testbed in Iran from which to perform network measurements. Our primary aim was to understand the mechanisms used for filtering in the country. To accomplish this, we analyzed traffic to blocked and non-blocked hosts at the packet level, and we used traceroutes to study hops inside the country's infrastructure. We conducted our primary measurements in the two months leading up to the June 2013 presidential election, when we expected censorship mechanisms to be aggressively deployed [4, 11]. Our results expose details of how traffic is being monitored and modified and provide an initial understanding of the censor's capabilities and limitations.

Although our study provides an initial technical perspective into mechanisms of censorship in Iran, it cannot be the final word on Internet freedom in the country. We probed the network from only one node at one ISP; while we observed that content blocking occurred exclusively at a centralized location in the national network, we cannot conclude that other ISPs do not apply additional layers of distributed filtering. Furthermore, our study spanned a period of only two months; Iran is known to adjust their censorship mechanisms frequently, and ongoing measurements are necessary in order to understand these changes over time. We hope to continue our probing and add additional collection points in order to present a broader perspective in future work.

*Pseudonymous authors.

Figure 1: Requests for censored sites are redirected to this page, located at http://10.10.34.34, which explains: "Access to the requested website is not possible. For complaints click here." After a 30 second delay, the user is forwarded to another censorship website, peyvandha.ir.

2 Background

The administrative hierarchy of Internet censorship in Iran is complex and includes many players. In March 2012, the supreme leader of Iran issued a directive establishing a new centralized agency responsible for managing the country's cyber policies known as the *Supreme Council of Cyberspace* [12]. This council controls three government bodies that are associated with censorship [20]:

- The *Committee for Determining Offensive Contents*, located at internet.ir and peyvandha.ir, which controls censorship policies in Iran. This committee is responsible for maintaining and updating lists of censored websites and also for enforcing internet communication policies.
- The *Iran Cyber Police*, or FATA Police, which is responsible for prosecuting users who are involved in illegal Internet activities as described by the Committee for Determining Offensive Contents.
- The *Revolutionary Guard Cyber Defense Command*, better known as the Iran Cyber Army, which is responsible for defending Iran against cyber attacks and implementing countermeasures.

Every ISP in Iran works under the jurisdiction of the *Communication Regulatory Authority of Iran* (CRA) [8], which enforces the censorship policies put in place by the Committee for Determining Offensive Contents.

Iran's government has been practicing Internet censorship for more than a decade. The first initiative to limit Internet access was issued by Iran's supreme leader in January 2002 in an order called the "Comprehensive Proclamation of Computer Information Network Policies" [22]. Initially, individual ISPs used IP address filtering to block access to certain "morally questionable" websites [29]. This system was later gradually replaced with a centralized system run by the state-run Telecommunication Company of Iran (TCI). Under this system, any web request to a blocked site is redirected to a web page owned by the censor, located at the address 10.10.34.34 (see Figure 1). This address, first established in March 2010 [2], is within private network address space as described by RFC 1918 [32] and is only accessible from inside Iran's national network.

The government has been observed to use a variety of techniques to control Internet access in the country:

Broadband speed limitations. Guidelines issued by the CRA [16] limit the bandwidth of home users to 128 kb/s. It is believed that this limitation is imposed to hinder access to multimedia content such as streaming audio and video. Researchers, faculty members, and university students are exempt from this limitation upon providing the appropriate documentation [16].

DNS redirection. DNS queries for some sites respond with a fake local IP address (10.10.34.34) that acts as a black hole.

HTTP host and keyword filtering. Authorities block access to certain prohibited sites by manipulating connections based on the HTTP `Host` header. Access to URLs containing certain keywords is also blocked. The list of prohibited keywords originally contained terms frequently used to access adult content, but it has been expanded in recent years in reaction to events causing political and economic turmoil, including presidential elections [40].

Connection throttling. In addition to these techniques, Iran has been observed to deploy connection throttling, particularly during times of political and economic unrest [40]. This has sometimes taken the form of throttling speeds to specific sites or protocols and sometimes complete throttling of all traffic [4]. Following the events of the presidential election in 2009, connection speeds to webmail services such as Gmail were reported to be significantly hindered [27]. Certain protocols, including HTTPS, SSH and VPN tunnels, have also been reported to be blocked or throttled at times [25].

It is believed that the Iranian government also has the capability to conduct **SSL man-in-the-middle attacks**. In 2011, an attacker who claimed to be Iranian compromised the DigiNotar certificate authority [30] and created hundreds of fake certificates for websites including google.com [30]. These certificates are reported to have

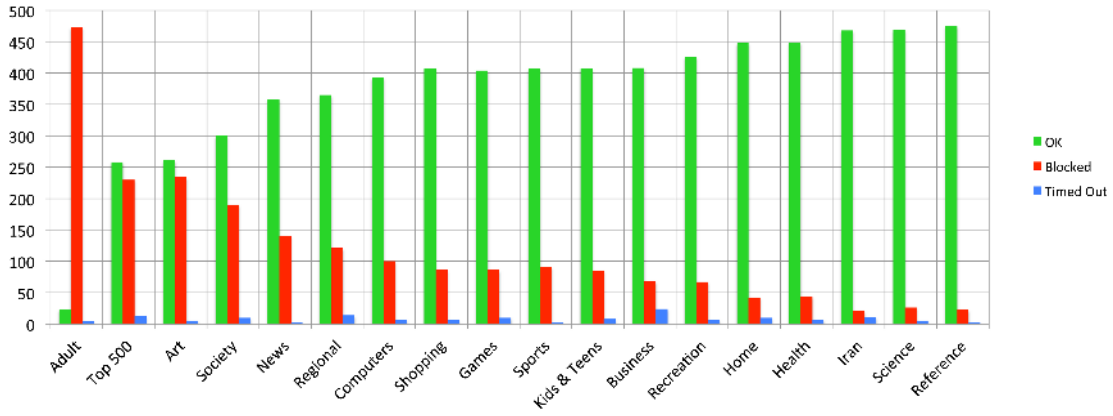

Figure 2: Effects of Iranian Internet censorship on the top 500 websites for 18 Alexa categories.

been used to initiate MITM attacks against more than 300,000 Internet users, almost all of them in Iran [30].

The most obscure aspect of Iran's censorship program is the network devices that allow traffic manipulation in such ways. It has been suggested that Iran relies on deep packet inspection (DPI) to selectively monitor and modify traffic [5, 26], but the locations, manufacturers, and full capabilities of these systems remain uncertain.

Iranian users have in turn used various types of anti-censorship tools to gain free access to the web [6]. Some of the widely used tools in Iran include Tor [41], Green Simurgh [15], FreeGate [13], Your Freedom [48], and Ultrasurf [43], as well as VPNs and SSH tunnels. In response, the censors have entered a cat-and-mouse game with these services to block users' access to them inside Iran. Many of the servers associated with these services have been blacklisted, and protocols associated with them have been blocked or throttled [25]. The Tor Project has detected DPI-based blocking being used against its service in multiple instances [28]. A malicious version of Green Simurgh infected with tracking software that records user activities has been reported in the wild [45].

3 Related Work

Most of the technical literature on Internet censorship has been focused on the Great Firewall of China (GFC). By necessity, we can give only a very brief survey here. Clayton et al. [7] address keyword filtering in the GFC, and Crandall et al. [9] claim that, contrary to previous belief, censorship in China does not occur only at the borders. Xu et al. [47] further explore the AS-level topology of China's network and manage to uncover many local firewall nodes inside China's infrastructure.

Other recent studies examining network topology and censorship mechanisms across many countries include discussion of Iran. In 2011, Roberts et al. mapped the autonomous systems (AS) of several different countries [36]. Their findings suggest that Internet traffic in Iran passes through a single "point of control." The following year, Verkamp and Gupta [44] looked at the mechanics of censorship in 11 countries around the world, including Iran. They conclude that censorship in Iran is hostname based and results in a 403 response followed by a redirection. Our work lends further evidence to support these findings.

Over the past year, Anderson performed the first technical studies dedicated to Internet censorship issues in Iran. In September 2012, he examined the use of private IP address space inside Iran's national network and found a large number of hosts in this space [3]. While our work was under review, Anderson released another report that looked at politically motivated Internet throttling in Iran [4]. He observed prolonged and significant disruptions in quality of service on dates associated with political or economic unrest. Our work complements these findings and is (to be the best of our knowledge) the first peer-reviewed technical publication focused on Iranian Internet censorship.

In a less technical vein, Reporters Without Borders has addressed Internet censorship in Iran [33], as have investigative journalists [24, 34], who cite data about devices that have facilitated DPI by Iran's government. The Iran Media Research program [21] and Small Media [37] have each issued reports on media censorship in Iran, emphasizing its social and humanitarian impacts.

4 Experiments and Results

The experiments we report below were conducted in April and May 2013, during the lead-up to the Iranian presidential election on June 14. We used a machine located inside Iran connected to one of the country's major ISPs. This

machine ran Ubuntu 12.10 (Quantal Quetzal). We refer to it by the codename *Aryan*; we have obfuscated any identifiable characteristics in our work to protect parties involved with this research inside Iran. In some of our experiments, we also used a second server outside Iran running Ubuntu 12.04 LTS (Precise Pangolin), Apache 2.2.22, OpenSSH 5.9p1, and BIND9.8.1p1. This host, which we refer to by the codename *Bob*, allowed us to monitor packets on both ends of the connection.

4.1 The Scope of Censorship

To evaluate the extent of censorship inside Iran, we surveyed the most-visited websites based on Alexa web traffic rankings. We created a crawler that retrieved the top 500 websites in each of 18 different Alexa categories and initiated a GET request from Aryan to these websites. The results of this experiment are illustrated in Figure 2.

The most censored category was, predictably, Adult websites, where more than 95% of sites were blocked. The most alarming was the overall Top 500 category, where more than 50% of the Internet's most visited websites were censored. Surprisingly, the Art category was the third most censored, followed by Society and News.

A breakdown of our results by blocking mechanism is presented in Table 1. DNS hijacking was observed only on domains associated with facebook.com, youtube.com, and plus.google.com. A number of website connections also timed out repeatedly when accessed from Iran. These sites generally belonged to sectors that are subject to U.S. government sanctions, such as banking (e.g., bankofamerica.com) and technology (e.g., nvidia.com), and some of them appear to block access from IP addresses in Iran.

We note that our study fails to cover many popular blocked Persian websites. These sites are not represented in Alexa's rankings for Iran as they are solely accessed using anticensorship software from inside the country and do not appear in other lists as they have little worldwide audience other than the small number of Persian speakers.

4.2 HTTP Host and Keyword Filtering

To probe the mechanism behind Iranian host-based filtering, we initiated HTTP requests from Aryan to blocked websites and examined the resulting network traffic. Figure 3 shows the typical network interactions related to this experiment. The three-way TCP connection handshake happens successfully between Aryan and the blocked website. However, when the GET request is sent from Aryan, it receives a packet containing an HTTP "403 Forbidden" error and an `<iframe>` containing the censorship page shown in Figure 1. We determined that this filtering is triggered by the `Host` header in HTTP requests. Omitting the header will circumvent host-based filtering but frequently results in a "400 Bad Request" response from the server. This behavior is consistent with earlier observations by Verkamp and Gupta [44] but differs from IP-based censorship practiced in China, which typically involves blackholing connections to the IP addresses of banned servers at the routing level [14].

		— Unreachable —			
Category	OK	Host	DNS	T/O	OK %
Adult	23	473	0	4	4.6
Top 500	258	227	3	12	51.6
Art	261	230	4	5	52.2
Society	300	190	0	10	60.0
News	358	140	0	2	71.6
Regional	365	120	1	14	73.0
Computers	393	97	3	7	78.6
Games	404	85	1	10	80.8
Shopping	407	86	0	7	81.4
Sports	407	91	0	2	81.4
Kids & Teens	407	85	0	8	81.4
Business	408	68	0	24	81.6
Recreation	426	67	0	7	85.2
Home	448	42	0	10	89.6
Health	449	44	0	7	89.8
Iran	468	19	2	11	93.6
Science	469	26	0	5	93.8
Reference	475	23	0	2	95.0

Table 1: Breakdown of top-500 websites' reachability in different Alexa categories. The Host column represent websites censored by means of HTTP `Host` filtering; DNS represents websites censored by DNS hijacking; and T/O represents sites that did not respond to our requests.

To examine how keyword filtering occurs, we created an empty HTML page named "sex.htm" on our remote server Bob. While an innocent page can be fetched successfully from Bob, visitors to this page are faced with a response similar to the host filtering case. When Aryan initiates an HTTP connection to fetch this page, it can complete the TCP handshake successfully with Bob, but upon sending the GET request, it receives an HTTP "403 Forbidden" response. Simultaneously, Bob receives 5 RST packets spoofed to appear to be coming from Aryan and closes its end of the connection. In our experiments, three of these packets had identical sequence number consistent with the TCP stream, while the other two had identical but seemingly random offsets from the previous three RST packet. This keyword filtering seemed to be limited to the HTTP request URI and did not cover POST data or the HTTP response body.

One way the censor might implement the filtering we observed is using a transparent HTTP proxy. To test this, we initiated a series of connections from Aryan to our external server Bob and compared the packets at both end-

points. We did not observe any anomalous changes in the TCP/IP headers, HTTP headers, or payloads that would indicate the presence of an intercepting proxy between the hosts, nor any suspicious patterns in connection timing. This suggests that a transparent proxy is not in use at the ISP we studied, and that the state-run filtering mechanism is based on another technology, such as DPI. However, other individual ISPs may have implemented their own transparent proxies to cache data or enforce more strict censorship policies [38].

4.3 DNS Hijacking

In our examination of Alexa top 500 websites, we encountered three domains (facebook.com, youtube.com, and plus.google.com) for which DNS responses directed the client to the censorship page IP address (10.10.34.34) instead of a valid IP address for the site.

To determine more precisely how these request were being blocked, we set up our own DNS server and initiated DNS requests from Aryan to it. Our observations suggested that blocked DNS queries never made it to our DNS server and were intercepted on path. In their place, our DNS server received 5 TCP RST packets spoofed from Aryan's address. In all of our experiments, three of these RST packets had an identical random sequence number while the other two had relative sequence numbers of 30 compared to the first three. This is a particularly curious result, since the original DNS queries were UDP packets and RST packets belong to TCP connections, and it may indicate that the censorship system is misconfigured. We also sent TCP DNS packets and observed no censorship on any domains. Figure 4 shows the interaction between Aryan and our DNS server.

4.4 Connection Throttling

To analyze the methods used to throttle connection speeds, we first measured the speed of file transfers from Bob to Aryan using the HTTP, HTTPS and SSH protocols. We used a file size that should have taken Aryan 96 seconds to download using its full bandwidth. We repeated this experiment mulitple times for each protocol.

For HTTP and HTTPS file transfers, Aryan used 85% and 89% of its total bandwidth on average, respectively. In contrast, for SSH file transfers, only 15% was utilized on average. All of our measurements were within 5% of these averages.

To confirm that this decrease resulted from the censor's interference, we proceeded to obfuscate our SSH file transfer (and therefore the unencrypted portion of its handshake) by XORing packet payloads with a predefined constant key. In this way, we expected to circumvent the censor's efforts to detect and throttle our SSH tunnel. Surprisingly, all of the trials using this modified SSH tunnel exhibited even worse performance. The obfuscated connection was constantly throttled to the point that download speed dropped to near zero at around 60 seconds into the connection. This resulted in incomplete file transfers during all of our trials.

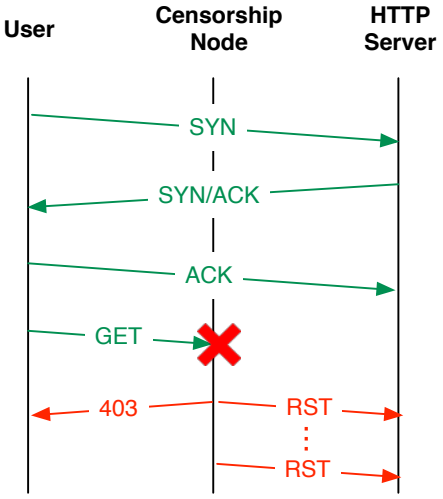

Figure 3: Network interaction between a user inside Iran and a blocked HTTP host. The same interaction happens if the URL of the page contains one of the keywords censored by the government.

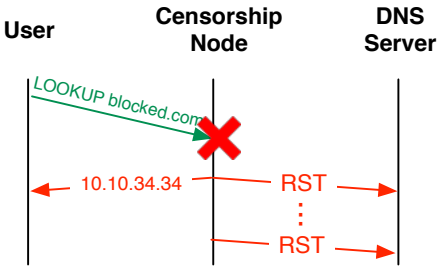

Figure 4: The process of DNS hijacking. The censorship node intercepts the DNS request and responds with an IP address serving a censorship page. It also sends unnecessary TCP RST packets to the DNS server.

From this observation, we hypothesize that instead of blacklisting undesired protocols, the censorship system was configured to whitelist approved protocols. This approach would allow the censor to preemptively block new, unrecognized circumvention techniques. It would also work to block Tor's obfsproxy protocol [42], which seeks to obscure identifiable features of the transport protocol. To test our theory, we used the obfuscation technique described above on HTTP file transfers. These experiments yielded results similar to the obfuscated SSH tunnel, supporting our protocol whitelisting hypothesis.

Our packet traces suggest that the throttling we observed was accomplished by dropping packets and causing TCP back-offs. Understanding the exact pattern and interval of these packet drops requires further investigation that we leave for future work.

Iran is known to vary its application of censorship technologies in connection with political and socioeconomic events, and the government has admitted throttling the Internet ahead of the June 2013 election [11]. We repeated our tests shortly after the election and found that connection throttling had been lifted from Aryan. SSH, obfuscated SSH, and obfuscated HTTP connections appeared to perform equally well, using an average of 82% of Aryan's bandwidth with a standard deviation of 5.5%.

4.5 Topology

To explore Iran's network topology, we first used ICMP traceroutes from Aryan to detect intermediate routers inside the country. We randomly chose 3160 destination IP addresses inside 13 neighboring countries using the IP address country block tool provided at IPInfoDB [18]. In our experiment, all of the observable first hops outside of the Iranian network were preceded by a node located at the private IP address 10.10.–.–, which we hypothesized was a device used for censorship. In each case, this node was preceded by one of two nodes owned by Telecommunication Company of Iran (TCI), which are the two paths used by Aryan's ISP to connect to the outside world. (We have omitted or partially redacted these addresses to prevent possible deanonymization of our ISP.) Figure 5 displays Aryan's view of Iran network topology.

Next we conducted an experiment to determine where along the path censorship functions were occurring, using a similar methodology to Xu et al. [47]. Aryan established a connection with a blocked website and sent GET requests with different IP TTL values. Depending on the response received by Aryan, we can determine if censorship is happening at this node or further along the path.

We established in Section 4.2 that the TCP handshake is not blocked by the censor, so we varied the TTL of the packet containing the HTTP GET request. When the TTL for our GET request expired before the suspected censorship node, we received an ICMP error. By incrementing the TTL from zero and recording the first "403 Forbidden" response, we confirmed that the suspected censorship node was indeed responsible for blocking our request. Similar experiments with DNS queries indicated that the same node was blocking them. We attempted to learn more about this censorship node by probing it with `nmap`, but it was unresponsive.

Additionally, we used Bob to traceroute to Aryan and to other IP addresses inside Iran. From Bob's point of view, the route to Aryan was the same as Aryan's route to Bob, except that Bob did not receive any response from the censorship node. Traceroutes to other IPs inside Iran similarly did not reveal the first hops inside Iran. Nevertheless, traceroutes to Aryan and to other Iranian IPs shared some of their Iran-based hops (after the missing hops), suggesting that a large amount of Iran's traffic passes through a centralized facility.

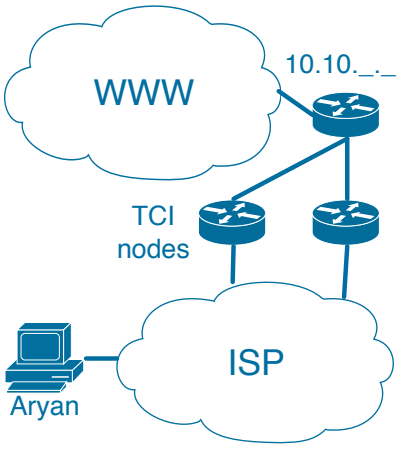

Figure 5: Aryan's view of Iran's network topology. The path from Aryan to the outside world (WWW) goes through one of two nodes owned by Telecommunication Company of Iran before passing the censorship node.

5 Future Prospects

Our study provides an initial technical perspective on the mechanisms behind Iranian Internet censorship, but a more complete understanding will require probing Iran's network infrastructure from multiple nodes inside the country, and monitoring the status of Internet access in Iran on an ongoing basis. Although we observed that at least some of Iran's censorship infrastructure is centralized, individual ISPs may be using additional mechanisms. Obtaining access to hosts located at many ISPs is necessary to allow researchers to explore such variations.

Similarly, even with the limited duration of our study, we were able to observe changes to connection throttling behavior before and after the June 2013 presidential election. Under special circumstances, Iran's government expands the restrictions imposed on users, including blocking access to the SSH protocol and webmail services entirely and performing SSL man-in-the-middle attacks. A longer study could lead to an understanding of the motivations and technical strategy behind such changes.

Based on Iran's history of aggressive Internet censorship, we consider it likely that the government will continue its efforts to monitor users and block anticensorship

techniques. Future work on next-generation anticensorship tools, such as Telex [46] and Cirripede [17], will be vital for achieving free Internet access among Iranian users in the face of increasingly sophisticated censorship mechanisms employed by the government.

6 Conclusion

In this work, we examined the status of Internet censorship in Iran. We studied how and where in the network censorship happens, and we measured the scope of the censorship by analyzing results for 18 categories of popular websites. We believe our results contribute to the efforts to understand how censorship is conducted in Iran and will be useful in the development of more robust countermeasures.

Of particular interest for censorship resistance is the centralized nature of the censorship mechanisms we observed. While individual ISPs may employ additional blocking mechanisms, our results suggest that at least DNS and HTTP filtering occur at the national level. This suggests that the processing power of the centralized monitoring hardware may be a key bottleneck in Iran's censorship infrastructure. New censorship resistance systems could explore techniques for overwhelming the central monitoring hardware with spoofed traffic, for instance, or for tunneling data past it and then further distributing it in a peer-to-peer manner within the country. We hope future work will build on our results to probe Iran's censorship infrastructure more deeply and to develop anticensorship mechanisms that maximally exploit its limitations.

Acknowledgments

The authors thank Eric Wustrow for discussions and advice on many aspects of this work. We also thank Collin Anderson and the anonymous reviewers for their insightful suggestions and comments. This work was funded in part by NSF grant CNS-1255153.

References

[1] The fifth five year development plan of the Islamic Republic of Iran. Chapter 4, Article 49. In Persian, 2011. http://ictb.ir/index.php/1389-12-02-12-27-38.

[2] Iran filtering webpage has changed. Gooya News Agency. In Persian, March 2010. http://news.gooya.com/politics/archives/2010/03/102519.php.

[3] Collin Anderson. The hidden Internet of Iran: Private address allocations on a national network. September 2012. http://arxiv.org/abs/1209.6398.

[4] Collin Anderson. Dimming the Internet: Detecting throttling as a mechanism of censorship in Iran. June 2013. http://arxiv.org/abs/1306.4361.

[5] Arseh Sevom. Breaking and bending censorship with Walid Al-Saqaf, February 2012. http://www.arsehsevom.net/2012/02/breaking-and-bending-censorship-with-walid-al-saqaf/.

[6] Cormac Callanan, Hein Dries-Ziekenheiner, Alberto Escudero-Pascual, and Robert Guerra. Leaping over the firewall: A review of censorship circumvention tools. Freedom House, May 2011. http://www.freedomhouse.org/sites/default/files/inline_images/Censorship.pdf.

[7] Richard Clayton, Steven Murdoch, and Robert Watson. Ignoring the great firewall of China. In *6th Workshop on Privacy Enhancing Technologies (PET)*, June 2006.

[8] Communication Regulatory Authority of Iran. http://en.cra.ir/.

[9] Jedidiah R. Crandall, Daniel Zinn, Michael Byrd, Earl Barr, and Rich East. ConceptDoppler: A weather tracker for Internet censorship. In *14th ACM Conference on Computer and Communications Security (CCS)*, 2007.

[10] Saeed Kamali Dehghan. Iran accused of torturing blogger to death. The Guardian, November 2012. http://www.guardian.co.uk/world/2012/nov/08/iran-accused-torturing-blogger-death.

[11] Golnaz Esfandiari. Iran admits throttling Internet to 'preserve calm' during election. Radio Free Europe, June 2013. http://www.rferl.org/content/iran-internet-disruptions-election/25028696.html.

[12] Farnaz Fassihi. Iran's censors tighten grip. The Wall Street Journal, March 2012. http://online.wsj.com/article/SB10001424052702303717304577279381130395906.html.

[13] Freegate. http://www.dit-inc.us/freegate/.

[14] Global Internet Freedom Consortium. The Great Firewall revealed, December 2002. http://www.internetfreedom.org/files/WhitePaper/ChinaGreatFirewallRevealed.pdf.

[15] Green Simurgh. https://simurghesabz.net/.

[16] Reza Hashemi. Iran to redefine broadband Internet. Cyber Persia blog, October 2010. http://asia.cnet.com/blogs/iran-to-redefine-broadband-internet-62114092.htm.

[17] Amir Houmansadr, Giang Nguyen, Matthew Caesar, and Nikita Borisov. Cirripede: Circumvention infrastructure using router redirection with plausible deniability. In *18th ACM Conference on Computer and Communications Security (CCS)*, pages 187–200, 2011.

[18] IPInfoDB. IP address country block generator. http://ipinfodb.com/ip_country_block.php.

[19] Iran Cyberpolice. http://www.cyberpolice.ir/.

[20] Iran Media Program. Internet censorship in Iran: An infographic, March 2013. http://iranmediaresearch.org/en/research/pdffile/1296.

[21] Iran Media Research. http://www.iranmediaresearch.org/.

[22] Iran Newspaper. Internet usage regulations will soon be announced, January 2002. In Persian. http://www.webcitation.org/5wUJOk7Fl.

[23] Sanja Kelly and Sarah Cook. Freedom on the Net 2011: A global assessment of Internet and digital media freedom. Freedom House, April 2011. http://www.freedomhouse.org/report/freedom-net/freedom-net-2011.

[24] Eli Lake. Fed contractor, cell phone maker sold spy system to Iran. Washington Times, April 2009. http://www.washingtontimes.com/news/2009/apr/13/europe39s-telecoms-aid-with-spy-tech/.

[25] Andrew Lewman. New blocking activity from Iran. Tor Project blog, June 2010. https://blog.torproject.org/blog/new-blocking-activity-iran.

[26] Andrew Lewman. Iran partially blocks encrypted network traffic. Tor Project blog, February 2012. https://blog.torproject.org/blog/iran-partially-blocks-encrypted-network-traffic.

[27] Elinor Mills. Gmail blocked in Iran ahead of protests? CNET News, February 2010. http://news.cnet.com/8301-27080_3-10451144-245.html.

[28] OONI Censorship Wiki. CensorshipByCountry/Iran. https://trac.torproject.org/projects/tor/wiki/doc/OONI/censorshipwiki/CensorshipByCountry/Iran.

[29] OpenNet Initiative. Internet filtering in Iran in 2004–2005: A country study, 2005. https://opennet.net/studies/iran.

[30] J. R. Prins. DigiNotar certificate authority breach "Operation black tulip", September 2011. http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf.

[31] Rahsa News Agency. Head of Cyber Defense Command: "National Internet should be launched as soon as possible", February 2012. http://www.rahsanews.com/archives/42289.

[32] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address allocation for private Internets. RFC 1918 (Best Current Practice), February 1996.

[33] Reporters Without Borders. Internet enemies report 2012, March 2012. http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf.

[34] Christopher Rhoads and Loretta Chao. Iran's web spying aided by Western technology. The Wall Street Journal, June 2009. http://online.wsj.com/article/SB124562668777335653.html.

[35] Christopher Rhoads and Farnaz Fassihi. Iran vows to unplug Internet. The Wall Street Journal, December 2011. http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html.

[36] Hal Roberts, David Larochelle, Rob Faris, and John Palfrey. Mapping local Internet control. In *25th IEEE Annual Computer Communications Workshop (CCW)*, 2011.

[37] Small Media. Iranian Internet infrastructure and policy report series. http://smallmedia.org.uk/.

[38] Small Media. Iranian Internet infrastructure and policy report (March-April 2013), April 2013. http://smallmedia.org.uk/InfoFlowReportAPRIL.pdf.

[39] Tabnak News Agency. Blocking of Gmail is an opportunity for national email service, February 2010. http://www.tabnak.ir/fa/pages/?cid=85319.

[40] Nitasha Tiku. Iran tries Internet censorship, execution as protesters demand democracy. New York Magazine, February 2011. http://nymag.com/daily/intelligencer/2011/02/iran_tries_internet_censorship.html.

[41] Tor Project. https://www.torproject.org/.

[42] Tor Project. obfsproxy. https://www.torproject.org/projects/obfsproxy.html.en.

[43] Ultrasurf. https://ultrasurf.us/.

[44] John-Paul Verkamp and Minaxi Gupta. Inferring mechanics of web censorship around the world. *2nd USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, August 2012.

[45] Chester Wisniewski. Spying Trojan targets Iranian and Syrian web surfers, dissidents. Naked Security blog, May 2012. http://nakedsecurity.sophos.com/2012/05/29/spying-trojan-targets-iranian-web-surfers-dissidents/.

[46] Eric Wustrow, Scott Wolchok, Ian Goldberg, and J Alex Halderman. Telex: Anticensorship in the network infrastructure. In *20th USENIX Security Symposium*, August 2011.

[47] Xueyang Xu, Z Morley Mao, and J Alex Halderman. Internet censorship in China: Where does the filtering occur? In *12th Passive and Active Measurement Conference (PAM)*, March 2011.

[48] Your Freedom. http://www.your-freedom.net/.