Bypassing Censorship: a proven tool against the recent Internet censorship in Turkey

Andrea Di Florio*, Nino Vincenzo Verde*, Antonio Villani†, Domenico Vitali*, Luigi Vincenzo Mancini*

* *Sapienza, Università di Roma*
Dipartimento di Informatica
{*mancini, verde, vitali*}*@di.uniroma1.it*
diflorio.1248896@studenti.uniroma1.it

† *Università di Roma Tre*
Dipartimento di Matematica
villani@mat.uniroma3.it

***Abstract*—Users of mobile devices are experiencing great difficulties to circumvent Internet censorship technologies that violate human rights. Mobile users do not have full control of their own systems, and in many cases, they cannot even change the configuration imposed by their 3G/4G providers. Such limitations allow the provider acting under the government authority to enforce specific Internet filtering mechanisms, and to prevent access to censored material.**

In this paper, we survey the events related to the Internet censorship happened in Turkey during the first months of 2014 and we introduce DNSet, an Android app that has been used by Turkish citizens to successfully circumvent the Internet censorship. In particular, DNSet allows mobile users to easily change the DNS server imposed by their 3G/4G providers, without the mobile users have administrative rights on the device (i.e. without rooting the device). We report on data and information that has been anonymously collected through the DNSet application. Furthermore, we raise up the suspicion that a few censorship activities in Turkey began at least a month before the official ban on Twitter.

***Keywords*-censorship; DNS; security; android; mobile; Turkey;**

I. Introduction

The Internet infrastructure has been conceived to allow everyone to access information from anywhere in the world. Nowadays, the Internet service is by far the fastest and unfettered carrier of information. Despite that, in the last decades, we have been seeing the Internet censorships performed by several governments. Chinese great Firewall (codename Golden Shield Project) [1] is one of the most famous censorship projects. Censorship techniques constantly change and they are implemented at each layer of the TCP/IP stack. In fact, whenever we touch a web services, or we query a social network, our devices perform several operations other than crossing a multitier stack of services. Each layer of this stack is susceptible to attacks and can be exploited for malicious purposes.

Since 2010, such attacks have been performed in many Countries, among others Egypt, Syria and Tunisia. In many of these cases, citizens suffered from a full censorship of the Internet network. For example, in 2011, Internet services were largely used by Egyptian anti-government activists to spread news to the entire world. Social networking systems such as Twitter and Facebook were the preferred means of communication, and they were used to help organize, communicate and launch civil-disobedience campaigns and street actions. In order to oppose such activities, Governments and Institutions accomplished explicit censorship by acting on the Internet infrastructure. In details, on January 2011, the Egyptian Security Intelligence Services ordered the blocking of Twitter. A few days later, the Internet censorship involved Facebook and the Egyptian Domain Name System (DNS). The GSM network and many Internet Services Providers became unstable as well. Many communication flows fell into a black hole: devices and users were fully disconnected from the networks. As a result, approximately 93% of all Egyptian networks were unreachable. In [2] the authors analyze episodes of the Egyptian and Libyan countrywide Internet disruptions that took place during the Arab Spring [3].

In early 2014, the Internet censorship in Turkey has focused on social networks. Initially, a DNS Tampering attack has inhibited Twitter and YouTube websites; later, their corresponding IP addresses have been blocked at the IP level. This censorship of the Internet can be easily bypassed by skilled PC-users. Specific network configuration or software tools can circumvent this kind of censorship when you are browsing the Internet with a PC. Unfortunately, mobile users cannot mitigate such attacks with the same simplicity. Usually, Android users do not have administrator-level permits on their devices. In order to obtain such privileged permits, they have to hack their own device. This procedure is called *rooting*. Rooting allows users to overcome carriers and hardware manufacturer limitations, enabling advanced settings, the utilization of a larger-set of applications and other operations that otherwise would be inaccessible.

The process of rooting an Android device does not come

for free: it may invalidate the device warranty, or even expose the device to many other vulnerabilities and attacks.

Contributions: The contributions of this paper are manifolds. First of all, we recall some censorship circumvention techniques and evaluate their effectiveness for the mobile scenario. Secondly, we survey the Internet censorship activities carried out by Turkey between February and April 2014, and we introduce *DNSet*, an Android app that has been used by Turkish citizens to successfully circumvent the censorship. Finally, we analyze data and information that have been collected during the censorship thanks to DNSet, and we raise up the suspect that a few censorship activities began at least a month before the beginning of the official censorship. As a matter of fact, our application was affected by a massive uninstallation problem, as reported by the information anonymously collected. It is worth mentioning that this is the first work showing some concrete evidence of such activity.

Organization of the paper: The paper is organized as follows: Section II reports on the censorship circumvention techniques available for the Android operating system and it describes the DNSet app; Section III summarizes the time line of the main Turkey censorship events and provides other contextual information, while Section IV introduces an analysis of the events supported by the data collected during those months. Finally, Section V provides the conclusions.

II. Circumvention of Internet censorship on Android

For the sake of this work, the *adversary* is an entity who wants to prevent any *victim host* from accessing an information on the Internet. We consider a powerful adversary, acting within an Internet Service Provider (ISP); she can modify the configurations of routers (e.g. modify the routing tables) and servers (e.g. DNS entries) in order to oversee and hijack all the traffic generated by the victims.

Internet censorship is performed through policies and technologies aimed at controlling access to information on the Internet [4]. In order to circumvent Internet censorship, several techniques were studied in the past. Unfortunately, only few of these techniques are suitable for smartphones, due to some restrictions implemented by vendors and providers. In this paper we focus on anti-censorship techniques that can be used on Android for two reasons: *i)* smartphones and tablets are largely used by people to access social networks or to coordinate themselves; *ii)* as far as we know, Android is now the most widespread Operating System for smartphones and tablets.

The most prevalent type of on line censorship is a method known as IP filtering. IP filtering is used to block or filter objectionable content by restricting access to specific IP addresses. To circumvent this method, the simplest countermeasure contemplates the use of a *proxy* server that is out of the adversary control (e.g. in a foreign country) [5], [6]. In this case, the victim host establishes a connection to the proxy server which forward the host's requests to the real destination. In such a way, the real destination of the traffic is encapsulated and remains unrevealed to the adversary. This countermeasure is suitable for Android since the user is allowed to configure a proxy server on Android. However, this countermeasure can be blocked by preventing the host from reaching the proxy server. More sophisticated anti-censor strategies improve this technique by adding a dynamic list of proxies. However, since such list only consists of a limited number of IP addresses, the adversary can discover, and block all the IP addresses in the list, preventing the victim from reaching the requested destination.

A more reliable way to circumvent IP filtering is Tor [7]. Tor is an overlay network that provides anonymity while surfing the web. Tor avoids censorship by forwarding encrypted packets between a randomly selected set of routers. Since the set of routers is randomly chosen, it is more complicated for the adversary to discover the actual destination of the packets. This feature makes Tor a more resilient countermeasure to censorship circumvention than proxies. The Tor client has been successfully ported on Android devices, and its implementation is called *Orbot* [8]. However, Tor has some drawbacks when it comes to the mobile scenario. First of all, some features which are available on the desktop version require root privileges on the mobile version. One of such features is the configuration of a transparent proxy. When configured in transparent proxy mode, *Orbot* is able to define a system-wide proxy and let other applications use the Tor network without even knowing it. Without the ability to configure a transparent proxy, apps must be properly modified/configured in order to use the Tor network. This is a strong limitation since, at the time of writing, only 7 applications of the Android market provide support for *Orbot*. To overcome these limitations, *Orbot* is able to run a proxy server on the loopback interface also. The user can configure a system-wide proxy for both Cellular and WiFi interfaces through the Settings menu of the Android system. Hence, the traffic generated by all the applications that use the system-wide proxy is anonymized. However, applications can bypass this type of proxy by using the `NO_PROXY` parameter when calling the method `getConnection()` of the class `java.net.URL`. Another important aspect that must be considered in the mobile scenario is the impact of anti-censorship countermeasures on the energy consumption. 3G network drains a large amount of power when a smart phone is in *suspended state* (i.e. the application processor is idle, while the communications processor is not) [9]. When it is used over 3G, *Orbot* maintains an active connection to the Tor overlay, draining the battery of a high-end smart phone in a few hours.

Another method for Internet censorship is DNS tampering [10]. The DNS is one of the most sensitive and critical

services of the Internet infrastructure. Each DNS server translates the human-readable address of a resource in the corresponding dotted decimal format. The DNS tampering attack happens whenever a user request receives a forged answer; this technique can redirect clients connections, and divert traffic flows. This method allows to block the access to specific contents by blocking the name of the site instead of the IP address. In order to do this, the adversary must control the DNS server used by the hosts. Previous studies showed that many countries implemented DNS censorship attacks [11], e.g. Malaysia, Russia and Turkey just to cite a few. In order to circumvent DNS tampering, the use of *public* DNS servers such as OpenDNS or Google DNS servers that are not under the control of the adversary may be sufficient. Still, the adversary can hijack the IP addresses of public DNS servers and prevent the hosts from correctly resolving hostnames.

It is worth mentioning that, in its basic configuration, neither Tor manages DNS queries nor it protects against DNS hijacking. If it is not properly configured, *Orbot* connects to the DNS server in the common way (i.e. without using the Tor overlay). This behavior deanonymize the destination and, above all, it does not prevent the adversary from hijacking the DNS. Things get worse on Android where the DNS server can not be easily modified. For such reason, we developed an app called DNSet that exploits a weakness of the Android system allowing the usage of an arbitrary DNS server without requiring root permissions [12].

A. DNSet

DNSet is an Android app that allows users to change the default DNS server imposed by their 3G/4G operators. The feature that distinguishes DNSet from many other Android apps is that it does not require root permissions. DNSet leverages on the *VPNService* package which is made available starting from Android 4.0 (Ice Cream Sandwich). This package allows android developers to establish their own virtual private network from within an application. In practice, the *VPNService* creates a new interface (called *tun0*), and allows the developers to set up the IP address, DNS servers, and the routing rules. Normally, developers should use the *VPNService* in order to establish a VPN connection with a remote server. Developers have to take care of forwarding all the outgoing packets to the *tun0* interface. In the same way, they have to manage all the incoming packets and forward them to the application level. DNSet does not use the *VPNService* in the conventional way. Indeed, DNSet establishes a fake *VPN* connection, it assigns a private IP address to the *tun0* interface (i.e. *10.10.10.2*), it sets two public DNS servers and, finally, it adds a very specific route to the routing table for the traffic that has to be forwarded to the *tun0* interface (i.e. *10.10.10.2/24*). As a consequence, the Internet traffic is not routed trough the *tun0* interface, but it continues to flow through the 3G/4G or WiFI interface. However, not only are the DNS servers set up in the VPN establishment phase used by the *tun0* interface, but they are also used by the other interfaces. This way, DNSet bypasses the impossibility to set up an alternative DNS server without having root permissions. It is worth noticing that the energy consumption of DNSet is quite negligible. As a matter of fact, after the initial setup of the "fake" VPN, DNSet does not have to care about incoming and outgoing packets.

As for August 2014, DNSet is used by more than 130 000 devices. Many of them are localized in Turkey (88%), a small part of them in Indonesia (7%), and the remaining 5% is spread around the world. Table I reports a detail of the geographic distribution of the devices that installed DNSet.

Table I
GEOGRAPHIC DISTRIBUTION OF THE DNSET APP AROUND THE WORLD, AS FOR AUGUST 2014

Country	Num. of Devices	Percentage
Turkey	115 750	88.41%
Indonesia	9 567	7.31%
Italy	2 342	1.79%
Malaysia	619	0.47%
United States	600	0.46%
United Kingdom	186	0.14%
Vietnam	109	0.08%
Germany	105	0.08%
India	99	0.08%
Canada	91	0.07%
Other	1 460	1.12%

III. THE TURKISH CENSORSHIP

In this section, we will summarize the main events of the Turkish censorship, and we will describe the *FATIH* project of the Turkeys Ministry of National Education that played a fundamental role in the circumvention of the censorship. A thorough analysis of the Internet Censorship in Turkey can be found in [13]. In this paper, the authors give an overview of the current legislative regime and provide a description of former content regulation and censorship examples. Unfortunately, the reported events in the paper do not consider attacks addressed to mobile devices that could be remotely controlled by the government.

A. The FATIH project

The FATIH project is a project of the Turkish government which seeks to integrate state-of-the-art computer technology into Turkey's public education system. On November 22nd, 2010, Prime Minister Recep Tayyip Erdogan started the project. The purposes of the FATIH project were put into practice the Smart Class, i.e. the Turkish government equipped more than 80 thousand classes of last mobile technologies for education aims. FATIH's first distribution phase began in the 2010-2011 school year in four schools. Each classroom in these schools was equipped with a laptop,

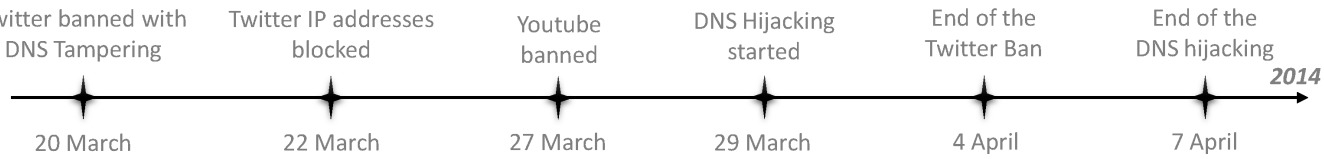

Figure 1. Time line of the main censorship events in Turkey (2014)

a projector, and an Interactive White board (IWB), that is a display system that projects images stored in a computer and allows users to control screen activities using a pen, stylus, or finger. Since 2011, at least 63 thousands tablets were distributed to Turkish students and 84 thousands classrooms were equipped as above. The tablet distribution process had a considerable deployment during the first months of 2014 [14].

The tablets distributed within the FATIH Project played a fundamental role during the Turkish censorship of March 2014. Indeed, they represented a large part of the mobile Internet enabled devices that were active at that time in Turkey. These devices are recognized as "Mehmet" by the Google Play Developer Console, that is the platform that enables developers to easily publish and distribute their applications directly to users of Android-compatible devices. By leveraging this platform, we have been able to collect several statistics and metrics about the DNSet app, extracting several information about the censorship events performed by the Turkish Government.

B. The censorship events

Figure 1 reports on the main censorship events happened in Turkey between March and April 2014. As it can be noticed, the Turkish government blocked Twitter on March 20th 2014. The government took this decision after the social media network had been used to spread recordings of telephone conversations and leaked documents that seemed to implicate high-ranking officials and some of their relatives and associates in a widespread corruption investigation [15].

The Turkish prime minister's office issued a statement before the ban was imposed, underlining the Twitters lack of cooperation after four local courts ruling that certain content had to be removed. The Twitter ban was initially based on the DNS Tampering technique. As a consequence of the Twitter ban, Turkish users started using alternative DNS providers such as Google DNS and OpenDNS servers, or manually resolving the Twitter IP address. As a response, on March 22nd, the Turkish government changed up its censorship strategy. In addition to the DNS tampering attack, the government blocked the IP of the Twitter servers within the Turkey networks.

Vijaya Gadde, the Twitter legal director for corporate and international issues, declared that the company, on March 26th, has been engaged in discussion with Turkish authorities about the removal of such content. She reported that the Turkish government requests were related to three distinct court orders: two of them were promptly removed since they violated Twitter rules as well; the third one was related to the closure of a Twitter account which had been used to make accusations of corruption against a former minister. Twitter decided not to remove it because, in their opinion, the removal was against the freedom of speech. To manage such a request Twitter used the "Country Withheld Content" tool. This tool allowed content to be withheld in a specific jurisdiction while remaining visible to the rest of the world [16].

On March 27th, the Turkish government banned the Youtube website[1] as well. The reason was a video claiming that the Turkeys foreign minister, the spy chief and a top general were discussing scenarios to lead their country's army attack jihadist militants in Syria [17].

After two more days, on March 29th, Turkey started to hijack the DNS traffic of alternative DNS servers. Essentially, the Turkish ISPs started advertising a more specific BGP route for OpendDNS servers and Googles Public DNS servers. For example, for the Google DNS server *8.8.8.8*, the Turkish ISPs advertised a specific route for *8.8.8.8/32* that went to their own network. Since a BGP router typically selects the most specific route as the one to be used to connect to a given IP address, all the connections on networks connected to Turkish ISPs would use this very specific route instead of the one advertised by Google, that is *8.8.8.8/24*. They apparently did this for all of Googles Public DNS addresses as well as those of other open public DNS providers. The Turkish ISPs went a step further: they set up their own DNS servers by answering as if they were actual public DNS servers in order to redirect the users to error pages for Twitter and Youtube websites.

The Twitter ban was revoked by the court on April 4th, so that the Twitter website became available again for the whole Turkey whereas the DNS hijacking remained active until April 7th.

IV. Analysis of the Turkish Censorship

In March 2014, Turkish citizens tried several techniques to circumvent censorship. TOR was one of the tools that

[1]The ban was revoked by a series of court rulings, starting on April 9, 2014. Turkey defied the court orders and kept access to YouTube blocked. On May 29th, the Constitutional Court of Turkey ruled that the block violated the constitutional right of freedom of expression and ordered to restore the access to the YouTube website.

allowed them to avoid the ban. Figure 2 reports on the number of Turkish clients connected to the TOR network from February to August 2014. It can be noticed that during the censorship the number of TOR clients has more than doubled, reaching almost 70 000 units. However, TOR does not represent a viable countermeasure for mobile devices for the reasons highlighted in Section II, and as a consequence people resorted to alternative countermeasures, such as VPN connections toward foreign countries and specific android apps such as DNSet.

Figure 3 reports on the number of Android devices with the DNSet app installed over time. In particular, it reports the total number of users that installed the app (indicated with *Total User installs*), the number of current DNSet users indicated with *Current User Installs* - this number considers also uninstallations - and the current number of devices with DNSet installed (indicated with *Current Device Installs*)- this number takes into account the fact that an individual user may own more than one device. It can be noticed that starting on March 20th, the number of DNSet users began growing extremely fast.

Many DNSet Turkish-users complained for a sort of automatic, unwanted, and unexpected uninstalls of the DNSet app. Figure 4 reports on the rate of uninstallations over installations in three different Countries: Indonesia, Italy and Turkey. A value greater than one means that the number of uninstallations were greater than the number of installations in that particular day. It can be noticed that around February and March there are several peaks of uninstallations; such peaks are all located in Turkey. We were not able to find a similar behavior in any other country.

Analyzing the data with more attention, we noticed that the number of uninstallations was very high only for a particular type of device, reported as "Mehmet" (i.e. the device belonging to the FATIH project). It has to be considered that on February 19th, 100 000 tablets were freely distributed to Turkish students within the Fatih program III-A, as reported in [18]. As for Mehmet devices, Figure 5 shows the ratio between uninstallations and installations of the DNSet app. Before February 22nd, DNSet was installed on 163 devices. We had no sudden variation on the ratio between uninstallations and installations. Contrary, from February 22nd to March 24th we noticed strange peaks of uninstallations. In particular, on February 22nd, in just one day more than 75% of Memhet users (i.e. 120 devices) uninstalled DNSet. Again, on March 21st more than 70% of Memhet users (i.e. 31 devices) uninstalled our app. These unusual activities stopped together with the first phase of the Twitter censorship, that is around March 22nd. From this day onward, the number of daily DNSet installations for Mehmet devices reached peaks higher than 2 000 units, with an average value of 892 daily installations. We do not have any actual evidence to say that the automatic uninstallations were executed by the Turkish government without the users approval, but our data confirm that some unusual uninstallation problem raised in Turkey approximately a month before the beginning of the censorship.

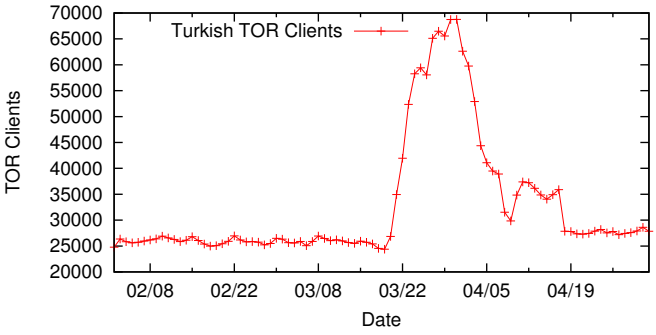

Figure 2. Turkish clients connected to the TOR network

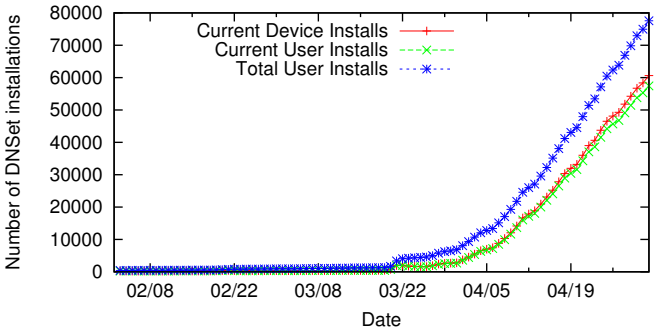

Figure 3. Number of DNSet Installations in Turkey

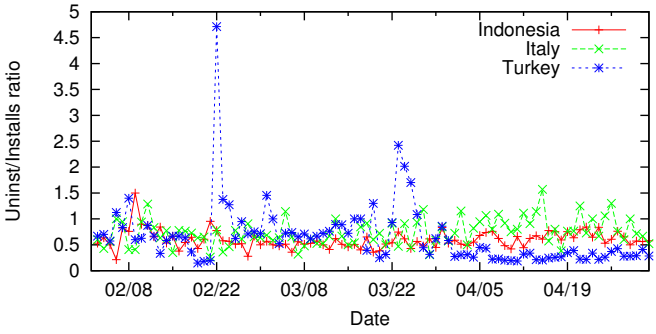

Figure 4. Rate of uninstallations over installations in different Countries

V. Conclusion

This paper analyzed the censorship events recorded between February and March 2014 in Turkey, and it introduced DNSet, a new Android app that is able to manage DNS configuration of mobile devices and mitigate one of the most widespread Internet censorship technique, i.e. the DNS tampering attacks. DNSet has been actually installed by

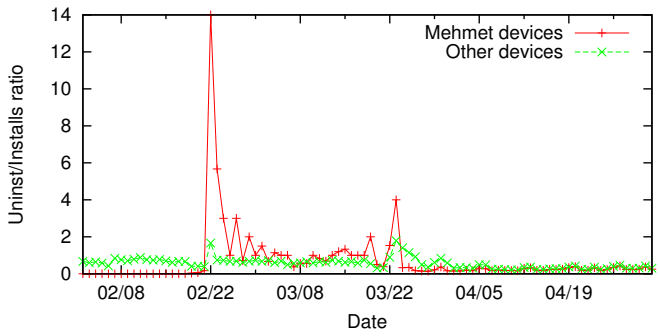

Figure 5. DNSet: Rate of uninstallations over installations of Mehmet Devices

more than 130 000 users in Turkey as for August 2014. Analyzing the data collected by DNSet we shed the light on a sustained campaign of boycott likely began a month before the official beginning of the censorship. We cannot confirm that such a boycott was preparatory to the Turkey's censorship, but we think that the scientific community should better investigate these events. As a matter of fact, to the best of our knowledge, it is the first time that a government leverages both the Internet infrastructure and a massive control of the end-user devices in order to perform a censorship.

ACKNOWLEDGMENT

This work has been partially supported by the TENACE PRIN Project (n. 20103P34XC) funded by the Italian Ministry of Education, University and Research, and by the European Commission Directorate General Home Affairs, under the GAINS project, HOME/2013/CIPS/AG/4000005057.

REFERENCES

[1] G. Lowe, P. Winters, and M. L. Marcus, "The Great DNS Wall of China," *Privacy Enhancing Technologies, Springer*, Dec 2007.

[2] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé, "Analysis of country-wide internet outages caused by censorship," in *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, ser. IMC '11. New York, NY, USA: ACM, 2011, pp. 1–18. [Online]. Available: http://doi.acm.org/10.1145/2068816.2068818

[3] S. P. Garry Blight and P. Torpey, "Arab spring: an interactive timeline of middle east protests," March 2011. [Online]. Available: http://www.theguardian.com/world/interactive/2011/mar/22/middle-east-protest-interactive-timeline

[4] C. S. Leberknight, M. Chiang, and F. M. F. Wong, "A taxonomy of censors and anti-censors part ii: Anti-censorship technologies," *Internation Journal of E-Politics*, vol. 3, no. 4, pp. 20–35, 2012.

[5] "Proxy dot org." [Online]. Available: https://www.proxy.org

[6] "Proxify." [Online]. Available: https://proxify.com/

[7] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, ser. SSYM'04. Berkeley, CA, USA: USENIX Association, 2004, pp. 21–21. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251375.1251396

[8] "Tor on android." [Online]. Available: https://www.torproject.org/docs/android.html.en

[9] A. Carroll and G. Heiser, "An analysis of power consumption in a smartphone," in *Proceedings of the 2010 USENIX Conference on USENIX Annual Technical Conference*, ser. USENIXATC'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 21–21. [Online]. Available: http://dl.acm.org/citation.cfm?id=1855840.1855861

[10] R. J. Deibert, J. G. Palfrey, R. Rohozinski, and J. Zittrain, *Access Denied: The Practice and Policy of Global Internet Filtering*. The MIT Press, 2008.

[11] J.-P. Verkamp and M. Gupta, "Inferring mechanics of web censorship around the world," in *Presented as part of the 2nd USENIX Workshop on Free and Open Communications on the Internet*. Berkeley, CA: USENIX, 2012. [Online]. Available: https://www.usenix.org/conference/foci12/workshop-program/presentation/Verkamp

[12] "Dnset app." [Online]. Available: https://play.google.com/store/apps/details?id=com.dnset

[13] Y. Akdeniz and K. Altiparmak, "A critical assessment of internet content regulation in turky," 2008. [Online]. Available: http://www.cyber-rights.org/reports/internet_restricted_colour.pdf

[14] E. R. I. (ERI), "Turkeys fath project: a plan to conquer the digital divide or a technologial leap of fatih?" December 2013.

[15] S. ARSU, "Turkish officials block twitter in leak inquiry," March 2014, [posted 20-March-2014]. [Online]. Available: http://www.nytimes.com/2014/03/21/world/europe/turkish-officials-block-twitter-in-leak-inquiry.html

[16] V. Gadde, "Challenging the access ban in turkey," March 2014, [posted 26-March-2014]. [Online]. Available: https://blog.twitter.com/2014/challenging-the-access-ban-in-turkey

[17] J. PARKINSON and E. PEKER, "Turkey muzzles youtube, media ahead of elections," March 2014, [Online; posted 27-March-2014]. [Online]. Available: http://online.wsj.com/news/articles/SB10001424052702304418404579465283912697784

[18] "Fatih project distributes tablets to ninth grade students by turkish company telpa," February 2014, [posted 19-February-2014]. [Online]. Available: http://www.turkishuschamber.org/index.php?option=com_content&id=3179