The State of Internet Censorship in Egypt

A research study by:
Open Observatory of Network Interference (OONI)
Association for Freedom of Thought and Expression (AFTE)

2nd July 2018

About

AFTE

The Association for Freedom of Thought and Expression (AFTE) is a non-governmental organization, registered in accordance with Egyptian law as a law firm since 2007. The association works to promote and protect freedom of expression and freedom of information. It uses research, legal support, monitoring of violations, and advocacy through its team of researchers and lawyers.

AFTE is concerned with a number of files, such as: media freedom, digital rights, freedom of information, freedom of creativity, academic freedom, student rights and freedoms, the right to privacy.

OONI

The Open Observatory of Network Interference (OONI) is a free software project under The Tor Project that aims to increase transparency of internet censorship around the world.

To this end, OONI develops free and open source software called OONI Probe, designed to measure various forms of network interference, such as the blocking of sites and instant messaging apps.

Hundreds of thousands of network measurements are collected from more than 200 countries every month, contributing to OONI Explorer, one of the world's largest publicly available resources on internet censorship.

Table of Contents

Authors

Mohammad El-Taher	Executive Director (AFTE)
Hassan Al-Azhary	Lawyer (AFTE)
Sarah Mohsen	Researcher (AFTE)
Leonid Evdokimov	Data Analyst & Backend Engineer (OONI)
Maria Xynou	Research and Partnerships Coordinator (OONI)

Probed ISPs

Most measurements collected from:

- Vodafone Egypt (AS36935)
- Link Egypt (AS24863)
- Telecom Egypt (AS8452)
- Noor (AS20928)

OONI Tests

- Web Connectivity
- HTTP Invalid Request Line
- HTTP Header Field Manipulation
- WhatsApp
- Facebook Messenger
- Telegram
- Vanilla Tor
- Tor Bridge Reachability

Testing/Analysis Period

January 2017 to May 2018

Censorship Methods

- Deep Packet Inspection (DPI) technology used to reset connections (HTTP response failures)
- DNS tampering
- TCP injections

Key Findings

Over the last year, internet censorship in Egypt appears to have become more dynamic and pervasive.

Egyptian ISPs don't seem to serve block pages, but reset connections through the use of Deep Packet Inspection (DPI) equipment. They also appear to be interfering with SSL encrypted traffic between Cloudflare's Point-of-Presence in Cairo and the backend servers of sites (located outside of Egypt).

Media websites make up most of the sites that we found to be blocked. More than 100 URLs that belong to news outlets appear to be censored, even though Egyptian authorities ordered the blocking of 21 news websites. Many human rights websites and blogs expressing political criticism were found to be blocked as well.

Circumventing internet censorship in Egypt can be challenging. Egyptian ISPs appear to be carrying out "defense in depth" tactics for network filtering, as suggested by the blocking of numerous circumvention tool sites. They also appear to be blocking access to the Tor network and, in some cases, Tor bridges. To block the site of a political party (Egypt's Freedom and Justice Party), ISPs use *two different* middleboxes, adding extra layers of censorship and making circumvention harder.

Egyptian ISPs appear to be carrying out an ad campaign. Back in 2016, we first found ISPs to be using DPI equipment to hijack unencrypted HTTP connections and redirect them to revenue-generating content, such as affiliate ads.

Our analysis of OONI measurements collected from Egypt over the last year strongly suggests that this campaign has been ongoing until (at least) March 2018. A wide range of different types of sites were affected, including news websites, human rights sites, LGBTQI sites, and UN sites (un.org and ohchr.org).

Introduction

This study is part of an ongoing effort to examine internet censorship in Egypt and in more than 200 other countries around the world.

The Open Observatory of Network Interference (OONI) and Egypt's Association of Freedom of Thought and Expression (AFTE) collaborated on a joint research study to examine internet censorship in Egypt through the collection and analysis of network measurements. The aim of our study is to document internet censorship in Egypt through the analysis of empirical data.

The following sections of this report provide more detailed information about Egypt's network landscape and internet penetration levels, its legal environment with respect to censorship and freedom of expression, as well as cases of censorship that have previously been reported in the country.

The remainder of the report documents the methodology and findings of this study.

Background

Network Landscape and Internet Penetration

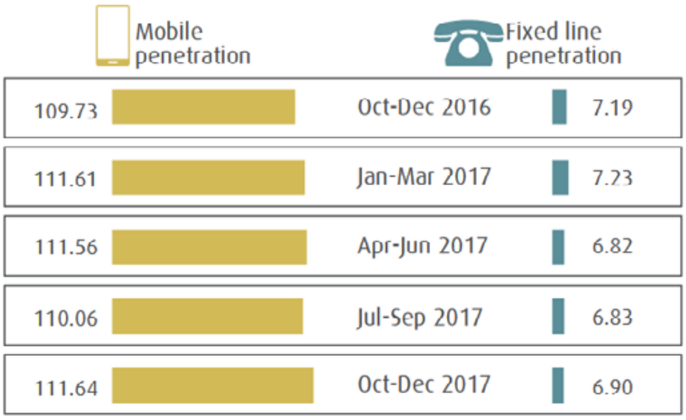
Access to the internet in Egypt has been increasing over the last years. According to the Ministry of Communications and Information Technology, the internet penetration rate in Egypt reached 41.2% by the end of 2017. This is largely based on mobile internet subscriptions, as illustrated in the following table.

Data item	Unit	Oct-Dec 2016	Jul-Sep2017	Oct-Dec 2017	Quarterly Growth Rate(%)	Annual Growth Rate(%)
ICT Sector:Infrastructure Indicators						
Mobile Subscriptions *	Million	97.79	99.40	101.27	1.88	3.56
Mobile Penetration **	%	109.73	110.06	111.64	1.58	1.91
Fixed Line Subscriptions	Million	6.12	6.54	6.60	1.02	7.95
Fixed Line Penetration **	%	7.19	6.83	6.90	0.07	-0.29
Mobile Internet Subscriptions	Million	28.65	32.76	32.79	0.09	14.45
USB Modem Subscriptions	Million	3.28	3.27	3.26	-0.30	-0.52
ADSL Subscribers	Million	4.44	4.95	5.20	4.94	17.1
International Internet Bandwidth	Gbps	1,134.25	1,406.12	1,536.12	9.25	35.43
Number of Post Offices	Post office	3931	3944	3946	0.05	0.38
ICT Sector's Role in Development						
Capacity Building Program Provided by ITIDA	Thousand Graduates	20.29	21.65	21.90	1.15	7.93

* Not including data of the fourth mobile service provider company (WE).
* * Growth rates are calculated as the difference between penetration rates in different time intervals.

Source: *Arab Republic of Egypt Ministry of Communications and Information Technology, Information and Communications Technology Indicators Bulletin: December 2017 (Quarterly Issue),* http://www.mcit.gov.eg/Upcont/Documents/Publications_142018000_EN_ICT_Indicators_Quarterly_Bulletin_Q4.pdf

By the end of 2017, most Egyptians accessed the internet via their smartphones, while fixed line subscriptions were limited to only 6.9% of the population. Over the last year, there is a noticeable decrease in fixed line penetration and an increase in mobile penetration, suggesting that Egyptians will continue to access the internet primarily on mobile networks.



Source: *Arab Republic of Egypt Ministry of Communications and Information Technology, Information and Communications Technology Indicators Bulletin: December 2017 (Quarterly Issue), http://www.mcit.gov.eg/Upcont/Documents/Publications_142018000_EN_ICT_Indicators_Quarterly_Bulletin_Q4.pdf*

Egypt has hundreds of Internet Service Providers (ISPs) which are regulated by the National Telecommunications Regulatory Authority (NTRA).

Vodafone Egypt enjoys the greatest share (40.5%) within the Egyptian mobile phone market, but state-owned Telecom Egypt owns a 45% share in Vodafone Egypt. Orange Egypt (owned by a French company) has a share of 33% in the mobile phone market, while Etisalat Misr (owned by an Emirati company) has a share of 24%. As for the fixed-line broadband market, Telecom Egypt controls 75% of the ADSL market.

In addition to owning a large share in Vodafone Egypt, state-owned Telecom Egypt also owns all of Egypt's telecommunications infrastructure. They lease licenses to Egypt's main ISPs - such as Noor, Etisalat Egypt, and Vodafone Egypt - who subsequently resell bandwidth to smaller ISPs. As a result, Egypt's internet infrastructure is quite centralized.

Legal Environment

Egypt's Constitution includes several provisions for the protection of press freedom and freedom of expression more generally. These provisions, however, can be restricted under certain conditions and under various Egyptian laws.

Constitutional Provisions

The Egyptian Constitution of 2014 guarantees access to information, protects press freedom and restricts censorship. According to Article 57 of the Constitution:

"The state shall protect the rights of citizens to use all forms of public means of communication, which may not be arbitrarily disrupted, stopped or withheld from citizens, as regulated by the law."

Article 68 of the Constitution guarantees the right to access information and official documents. More specifically, it states:

"Information, data, statistics and official documents are owned by the people. Disclosure thereof from various sources is a right guaranteed by the state to all citizens. The state shall provide and make them available to citizens with transparency. The law shall organize rules for obtaining such, rules of availability and confidentiality, rules for depositing and preserving such, and lodging complaints against refusals to grant access thereto. The law shall specify penalties for withholding information or deliberately providing false information."

Based on this Article, Egyptian authorities can be compelled to disclose judicial or administrative decisions on censorship. Article 71 of the Constitution protects press freedom and prohibits media censorship (though it can be justified during war or in times of general mobilization):

"It is prohibited to censor, confiscate, suspend or shut down Egyptian newspapers and media outlets in any way. Exception may be made for limited censorship in time of war or general mobilization."

Emergency Law

During a state of emergency, constitutional rights are suspended. Egypt's Emergency Law allows the government to intercept and monitor all communications, impose censorship and confiscate publications.

Under Article 3 of this law, authorities can monitor letters, newspapers, publications, editions, drawings and all other means of expression, prior to their dissemination. They are also authorized to control and expropriate them, and to shut down the places where such publications are printed (such as the offices of newspapers). Article 3 of Egypt's Emergency Law could potentially be referenced to justify the blocking of websites.

Egypt has been in a state of emergency since 1958 (when the Emergency Law was first issued), except for a few short breaks. In recent years, the longest period *without* a state of emergency lasted for 13 months, from July 2012 to August 2013. Over the last decades, Egypt has almost constantly been in a state of emergency through the continuous issuance of decrees that extend it. More recently, the Egyptian government declared a state of emergency in April 2017, following two church bombings that killed at least 44 people. A year later in April 2018, the government issued its fourth decree to extend the state of emergency for another three months.

Anti-Terrorism law

Three years ago, in 2015, Egypt adopted an anti-terrorism law which imposes a fine for publishing reports that contradict official accounts of militant attacks. Critics of the law have argued that it could potentially be used to shut down small newspapers and to deter larger ones from reporting on attacks and operations against armed fighters.

Under Article 29 of this law, the Public Prosecutor (or the relevant investigating authority) is authorized to *block websites* that commit criminal offences, such as inciting violence or spreading terrorist messages.

Telecommunications Regulatory Law

Telecommunications in Egypt are centrally administered, potentially enabling centralized internet censorship.

Article 67 of Egypt's Telecommunications Regulatory Law allows authorities to administer all telecommunications services and networks of all operators and service providers in light of environmental disasters, general mobilization, or to preserve national security. In such cases, this law can enable authorities to implement internet censorship in a centralized way.

According to AFTE, Egyptian authorities referred to this law to censor communications and internet services during the Egyptian revolution in January 2011 on the grounds of national security.

In extension of Article 67, Article 68 of the law aims to exempt service providers from the scope of liability and to even compensate them for any damages that may occur as as result of government network management. Recently, however, Egypt's Parliamentary Committee of Communications approved Article 31 of the draft Cyber Crime bill. This Article aims to punish Internet Service Providers (ISPs) who refrain from blocking websites that "threaten national security" according to court orders.

Cyber Crime Bill

Egypt's Parliament recently approved the Cyber Crime Bill, legalizing the blocking of websites and expanding upon surveillance powers.

Article 7 of the Bill authorizes the investigative authority to block websites when it considers that the content published on these sites constitutes a crime or threat to national security or jeopardizes the security of the country or its national economy. The investigative authority presents the matter to the competent court within 24 hours and the court shall issue its decision within a period not exceeding 72 hours either by acceptance or rejection.

Article 7 then expands on granting the authority to issue a blocking decision, giving the right to investigation and enforcement authorities (the police) to inform NTRA to immediately notify service providers of the temporary blocking of the sites. The order has to be immediately executed upon receipt. As with all provisions of the Cyber Crime Bill, which is rife with vague terms that can include anything, the power to issue a blocking order is given to investigation and enforcement authorities in ***"cases of urgency caused by imminent danger or damage."***

It is noted that the investigation and enforcement authorities have the authority to issue a decision to implement a block without the need for prior permission.
Then the decision is presented by investigation bodies to the court within 24 hours; and then the court issues its decision in a period not exceeding 72 hours either by acceptance or rejection. The decision of investigative authorities is neither enforced nor implemented, except after a judicial decision is issued by the competent court.

The law does not give any definition or clarification of what may be considered by the investigative authorities to jeopardize the security and economy of the country. These accusations were previously directed against many of the demonstrators and activists in investigations and trials. The calls for demonstrations were considered a threat to national security. In the foreign funding case no. 173 activities of independent civil society organizations were considered a threat to national security and the safety of the country.

While the law does not define the threat to the country's security and economy, it provides a broad definition of national security which includes all aspects of independence, stability and security of the homeland and its unity and safety, of its territory, affairs of the Presidency, the Council of Defense, the National Security Council, the armed forces and military production, the Ministry of the Interior, the General Intelligence, the Administrative Oversight Authority, and the organs affiliated to those bodies. This definition can not include everything published by any of the mentioned entities on social media, news sites or any sites that publish content contrary to the authority's policies.

Although Article 5 of the Explanatory Note protects personal data of users, the following provisions of the law entrench comprehensive surveillance over all users of telecommunications services in Egypt.

Article 2 of the law requires telecommunications companies to keep and store customer usage data for 180 days, including data that enables user identification and data relating to the content of the information system, the movement of the user and the devices used. This means that telecom providers will have data that describes all user practices, including phone calls and text messages, and all related data, websites visited and applications used on smartphones and computers.

Article 5 also requires telecommunications companies to comply with any ***"other data to be determined by a decision"*** from the NTRA board, which means that telecommunication providers can be obliged to collect and retain data not provided for in the law, but only upon an administrative decision issued by the NTRA. The article grants the right to national security authorities to view these data and obliges providers of telecommunications services to provide the technical assistance for this.

The article stipulates that “the service providers and their subordinates shall, in the event of a request by national security authorities and according to need, provide those authorities with all available technical facilities so that they may exercise their mandate in accordance with the law.”

The Act defines national security bodies to include the Presidency, the Armed Forces, the Ministry of the Interior, the General Intelligence and the Administrative Oversight Authority. Article 5 does not address any details linking surveillance with any of the crimes mentioned in the law, but imposes comprehensive surveillance on all users in Egypt.

While Egyptian citizens already have many problems with having to disclose their personal data in their normal daily practices, the article expands the authority to collect user data, requiring “IT service providers, their agents and distributors who market these services to obtain user data”. This practice is already in existence and caused chaos in the use of personal data of citizens.

Egypt has no laws concerning the protection of personal data. During the past year, AFTE documented several cases in which some distributors used personal data of users without their knowledge, including the sale of mobile phone lines. As a result, in many cases, personal accounts were compromised on social networks and e-mail, and all services associated with them have been compromised as the use of ICT in business and financial transactions grows, as well as subjecting them to prosecutions in case any telecommunications services were used to commit a crime punishable by law.

In the same context, the text of Article 4 of the law deals with the exchange of data and information between Egypt and foreign countries through the Ministries of Foreign Affairs and International Cooperation within the framework of international, regional and bilateral agreements or the application of the principle of reciprocity, without defining the conditions for this exchange of information, particularly concerning the existence of data protection laws in other countries or requirements regarding the scope, duration of retention or processing of information.

Access to Information Law

Since the establishment of the right to access information in the Egyptian Constitution issued in 2012 and the current Constitution issued in 2014, a number of drafts on the Access to Information Law have been prepared. The last of these drafts issued by the Committee, which was formed through the Supreme Media Council, was submitted to the Egyptian Cabinet in late 2017 in preparation for its discussion in parliament. However, since its submission, the draft has not been discussed yet.

During recent government practices, including the blocking of websites, the Supreme Media Council formed a committee to draft a law to access information pursuant to the constitutional provision stipulated in Article 68 of the Egyptian Constitution. The committee completed drafting a law in October 2017, consisting of 28 articles regulating the concept of the right to access information, the scope of exceptions related to information and data that are not accessible, the formation of a higher information council, the nature of offenses, and offenses related to access to information and their penalties.

The draft was submitted to the Egyptian Cabinet in preparation for its discussion in parliament. However, since its submission, the draft has not been discussed yet.

Reported cases of Internet Censorship

Unlike other countries in the region, few internet censorship events were reported in Egypt in the years following the 2011 revolution. In late 2015, however, things changed. Along with Saudi Arabia and the United Arab Emirates, Egypt reportedly blocked access to Al-Araby Al-Jadeed, a Qatari-owned news website. The blocking was justified on the grounds of the site "serving as a mouthpiece of the Muslim Brotherhood" and in light of escalating tension in the region.

Network measurement data collected through the use of OONI Probe not only confirmed the blocking of Al-Alarby, but also showed that an alternative domain (alarabyaljadeed.co.uk) set up for censorship circumvention was also blocked. OONI reported that the blocking of Al-Alarby resulted in collateral damage, since other websites hosted on the same Content Delivery Network (CDN) were found to be blocked as well.

Soon thereafter, Egypt started blocking a variety of news outlets. On 24th May 2017, the Egyptian government ordered ISPs to block 21 news websites on the grounds of “supporting terrorism and lies”. Through the collection and analysis of network measurements, OONI identified the blocking of ten news websites - including local and international news, such as Mada Masr and Aljazeera. OONI also found the Tor anonymity network, the Tor domain, Tor bridges, and their *own* website - which is a Tor subdomain - to be blocked in Egypt as well. But this was not the first time OONI noticed that access to the Tor network was interfered with in Egypt. In 2016, OONI reported on attempts by Egyptian ISPs to block access to the Tor network.

In an attempt to identify all 21 blocked news outlets and to investigate further, AFTE collected more network measurements through the use of OONI Probe across multiple ISPs in Egypt. They subsequently published two research reports on the blocking of (at least) 496 websites, suggesting that internet censorship in Egypt has now become *pervasive*. These blocked sites expand beyond news outlets, also including human rights websites, circumvention tools, blogs, publishing platforms, the sites of political movements, social networks, and wikis, among other types of websites.

According to AFTE, the blocking of media websites is in violation of Article 57 of the Constitution, which states that it is not permissible to suspend the means of public communication arbitrarily. AFTE also asserted that the block is in violation of a number of administrative and constitutional courts, as well as of the Universal Declaration of Human Rights and a number of United Nations resolutions and charters that the Egyptian government is committed to.

More recently, AFTE published another research report on the blocking of Accelerated Mobile Pages (AMP) in Egypt, affecting millions of others websites that use it. AMP improves the performance of webpages on mobile phones, providing a faster and better experience for smartphone users. In Egypt, many owners of blocked websites adopted AMP as a censorship circumvention strategy.

Since AMP serves alternative links to the original links that appear on Google search, users are redirected to an alternative domain, circumventing the blocking of the original site.

By blocking AMP, Egyptian authorities not only make censorship circumvention harder for blocked sites, but they also affect millions of other websites that use AMP merely for the purpose of providing better web performance to their smartphone users.

This is one of various cases where censorship practices in Egypt have led to collateral damage. In 2016, OONI reported on the HTTPS throttling of services hosted by DigitalOcean's Frankfurt data centre, leading to the inaccessibility of various URLs. As part of this report, OONI also uncovered an ad campaign. State-owned Telecom Egypt was found to be using Deep Packet Inspection (DPI) technology (or similar networking equipment) to conduct man-in-the-middle attacks to inject content for gaining profit (affiliate advertising) or malicious purposes (to serve malware).

Recently, the Citizen Lab expanded on this research by investigating the use of Sandvine/Procera Networks DPI devices for malicious or dubious ends in Egypt, Turkey, and Syria. As part of their research, they found that middleboxes were being used in Egypt to hijack users' unencrypted connections and redirect them to revenue-generating content, such as affiliate ads and browser cryptocurrency mining scripts.

The Citizen Lab also found that devices, matching their Sandvine PacketLogic fingerprint, were being used to block dozens of political, human rights, and news websites in Egypt, including Human Rights Watch, Reporters Without Borders, Al Jazeera, Mada Masr and HuffPost Arabic.

Methodology: Measuring Internet Censorship in Egypt

To measure internet censorship in Egypt, we ran OONI's network measurement software (called OONI Probe) on a daily basis across multiple local vantage points. OONI Probe is free and open source software designed to measure various forms of network interference.

The main OONI Probe tests that we ran as part of this study include:

- Web Connectivity
- HTTP Invalid Request Line
- HTTP Header Field Manipulation
- Vanilla Tor
- Tor Bridge Reachability
- WhatsApp
- Facebook Messenger
- Telegram

Given that the Egyptian government ordered the blocking of 21 news websites, running OONI's Web Connectivity test was core to this research to collect network measurement data that shows which websites are blocked, how they are blocked, and which ISPs implement the blocks.

OONI's Web Connectivity test is designed to measure whether websites are blocked by means of DNS tampering, TCP/IP blocking, or by an HTTP transparent proxy. This test is automatically performed both over the vantage point of the user and from a non-censored control vantage point. If the results from both vantage points match, then the tested website is most likely accessible. If the results however differ, then the measurement is flagged as anomalous. OONI's current methodology only confirms the blocking of a website if a blockpage is served. In cases where ISPs do not serve blockpages, the relevant network measurements are analyzed over time, examining whether the specific types of failures persist and what causes these failures (i.e. ruling out false positives).

The testing was mostly limited to the URLs included in the Citizen Lab's global and Egyptian test lists.

These lists consist of a variety of different types of URLs that fall under 30 categories and that are tested for censorship by network measurement projects like OONI. Throughout the course of this research, we updated the Egyptian test list several times to ensure that reportedly blocked sites were being tested. Overall, 1,808 URLs, included in both the Citizen Lab's global and Egyptian test lists, were measured as part of this study.

In an attempt to identify which equipment was used to implement internet censorship in Egypt, we ran OONI's HTTP Invalid Request Line and HTTP Header Field Manipulation tests. Both tests are designed to measure networks with the aim of identifying the presence of middleboxes. OONI's HTTP Invalid Request Line does this by sending an invalid HTTP request line to an echo server listening on the standard HTTP port. If a middlebox is present, the invalid HTTP request line will be intercepted by the middlebox, potentially triggering an error that will be sent back to OONI servers.

In the past, this has enabled the identification of censorship equipment in various countries around the world. OONI's HTTP Header Field Manipulation test, on the other hand, attempts to identify middleboxes by sending HTTP requests with non-canonical HTTP headers. If a middlebox is present, it will likely normalize the headers or add extra headers, enabling the identification of its presence in the network. In addition to OONI Probe tests, we also performed latency tests and other network measurement tests via Raspberry Pi deployments in Egypt.

To monitor the accessibility of popular instant messaging platforms over time, we ran OONI's WhatsApp, Facebook Messenger, and Telegram tests. These tests are designed to measure the reachability of the WhatsApp, Facebook Messenger, and Telegram apps and web interfaces through DNS lookups and by attempting to establish TCP connections to their endpoints.

In light of increased censorship events over the last year, we decided to monitor the accessibility of censorship circumvention tools as well. Many circumvention tool sites were included in the Citizen Lab's global test list, which we measured via OONI's Web Connectivity test.

But we also ran OONI's Vanilla Tor and Tor Bridge Reachability tests, which are designed to measure the blocking of the Tor network and Tor bridges.

Once network measurement data was collected from all of these tests, OONI data was subsequently processed and analyzed based on a standardized set of heuristics for detecting internet censorship and traffic manipulation. We analyzed all OONI Probe network measurements collected from Egypt between January 2017 to May 2018.

Acknowledgement of Limitations

The findings of this study present limitations. The first limitation is associated with the testing period. This study includes an analysis of hundreds of thousands of network measurements collected from networks in Egypt between January 2017 to May 2018. Censorship events that may have occurred before and/or after the analysis period are not examined as part of this study.

Another limitation to this study is associated to the amount and types of URLs that were tested for censorship. OONI's Web Connectivity test was run to measure the accessibility of 685 URLs that are more relevant to the Egyptian context and 1,123 internationally relevant sites. All of these URLs were selected and categorized in collaboration with community members over the last years.

We acknowledge that some URLs might potentially be mis-categorized, the selection of the URLs may have been biased, and that the testing sample of URLs might exclude many other sites that are blocked in Egypt. We therefore encourage researchers and community members to continue reviewing and contributing to these test lists to help improve future research and analysis.

Finally, while network measurements were collected from multiple local vantage points in Egypt, OONI's software tests were not run consistently across all networks. We therefore limited most of our analysis to the networks where measurements were collected from the most (allowing for more accurate data analysis over time): Vodafone Egypt (AS36935), Link Egypt (AS24863), Telecom Egypt (AS8452) and Noor (AS20928).

Findings

Blocked Websites

Egyptian ISPs do not appear to implement block pages (at least for none of the tested sites), limiting our ability to confirm censorship events with absolute confidence.

To examine the blocking of websites, we analyzed all of OONI's Web Connectivity measurements collected from local vantage points in Egypt between January 2017 to May 2018. As part of our analysis, we examined which websites presented network anomalies, whether those network anomalies were consistent and persistent over time, and whether those sites had high global failure rates (as part of efforts to rule out false positives). Overall, 1,054 URLs presented network anomalies and signs of network interference throughout the testing period of this study. Many of these sites, however, were accessible most of the times that they were tested, suggesting that some of the failures were either false positives or that those sites were only temporarily blocked.

We narrowed our analysis to the URLs that consistently presented a high amount of network anomalies (e.g. HTTP failures) in comparison to the total amount of times that they were tested over time. We subsequently filtered out many URLs that had expired or squatted domains. Such URLs may have been blocked (given that they presented a high ratio of network anomalies), but we decided to exclude them from this study since they are no longer operational anyway (limiting the impact of their potential censorship). This left us with 181 URLs that consistently presented the same types of anomalies most of the times that they were tested across multiple ISPs over time, strongly suggesting that they were inaccessible in Egypt.

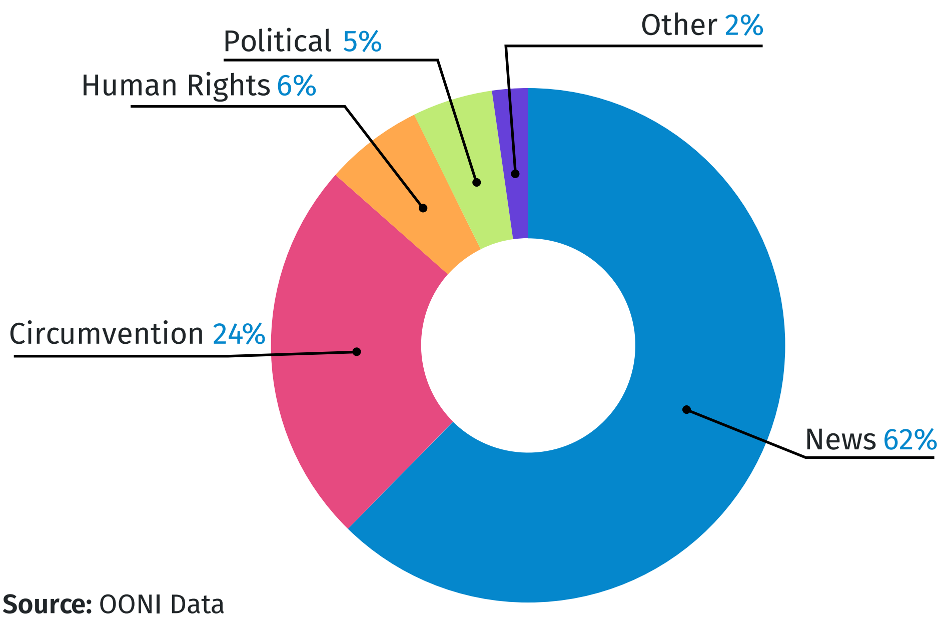
These 181 URLs, however, include 3 Israeli domains (isa.gov.il, iaf.org.il, mod.gov.il) that don't appear to be blocked by Egyptian ISPs, but by Israel. There is no common policy in terms of how they're blocked. The nameserver for isa.gov.il does not respond to Egyptian IPs, access to iaf.org.il from Egypt is blocked on the IP level, while mod.gov.il appears to be inaccessible in Egypt due to geographic-based restrictions. Excluding these 3 Israeli sites, a total of **178 URLs** appear to most likely have been blocked by Egyptian ISPs, given that they were tested hundreds of times across multiple networks, and consistently presented a high ratio of network failures.

These sites primarily appear to be blocked through the use of **Deep Packet Inspection (DPI) technology which was used to reset connections**, leading to HTTP response failures.

Over the last year, internet censorship in Egypt appears to have become quite *pervasive*, since many different types of sites appear to be blocked. The chart below illustrates the types of sites that presented the highest amount of network anomalies and are therefore considered to more likely have been blocked.

Blocked websites in Egypt

Categories of blocked websites



Source: OONI Data

Most of the censored sites include *news outlets*, followed by a number of circumvention tool sites, human rights sites, and several blogs and sites that express political criticism.

In May 2017, the Egyptian government ordered the blocking of 21 news websites, but our analysis suggests that *more than 100 news websites* may have been blocked over the last year. A considerable amount of sites hosting human rights content and views expressing political criticism presented a high ratio of anomalies as well, indicating that the censorship may have been politically motivated. The fact that many circumvention tool sites also presented a high ratio of network anomalies suggests that Egyptian ISPs may have attempted to reinforce their censorship by making circumvention harder.

It's worth noting that the above chart presents limitations, particularly since it's determined by the amount and types of websites that were tested as part of this study. If a different sample of websites was tested, the chart would have probably been different. Nonetheless, the aim of this chart is to show which types of sites presented the highest amount of anomalies within the constraints of the specific lists of websites that were tested.

The following sections dive into the four categories of sites (news, human rights, political criticism, and censorship circumvention) that presented the highest ratio of anomalies as part of this study, and which therefore are more likely to have been blocked during the testing and analysis period of this study.

News Outlets

Media websites make up the vast majority of the sites that we found to be blocked as part of this study.

Out of the 178 blocked URLs, 111 of them belong to various news outlets. These URLs were tested hundreds of times, and consistently presented a high ratio of HTTP failures throughout the testing period. The full list of blocked news websites, illustrating the amount of times they were tested versus the amount of times they presented HTTP failures, is available **here**.

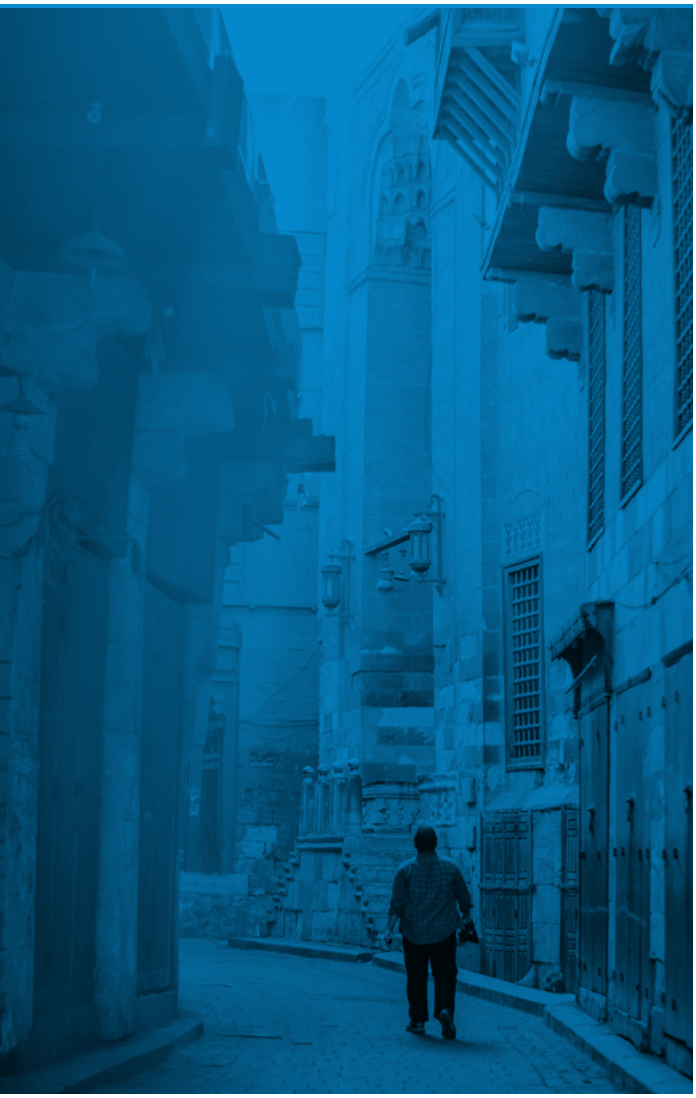
The blocked URLs include local Egyptian news outlets, as well as international media websites. These include Mada Masr, Al Jazeera, Rassd News Network, Sasa Post, Al-Araby Al-Jadeed, Daily News Egypt, Huffington Post Arabic, Al Borsa News, Almesryoon and Masr Al Arabia, among many others. Overall, more than 100 media websites appear to have been blocked throughout the testing period, and this finding is limited to a relatively small sample of media outlets that were tested.

It's worth noting that we found various Turkish and Iranian news websites to blocked (such as turkpress.co, turk.life and arab-turkey.com for Turkey, and alalam.ir for Iran), suggesting that politics and security concerns may have influenced censorship decisions. The blocked news websites also include a sarcastic website (alahraam.com) and a Qatari-owned news outlet (qtv.qa), among other regional and international news websites.

Lebanese newspaper Al Akhbar was blocked following the publication of news involving the resignation of the director of the Egyptian General Intelligence.
The site of "Fi Al-fann", the largest site providing cinema news, was blocked after

publishing news about Turki Al Sheikh (an adviser in the Royal Court of Saudi Arabia) beating an Egyptian singer. Cairo 24 news outlet was blocked after publishing a report on the attack on Hisham Genina, one of the opponents of the current regime.

News website Sout Al Omma was temporarily inaccessible in June 2017. Given that OONI measurements show a connection timeout error, the site may have been DDoSed, particularly since Cloudflare couldn't establish a connection to the backend server of the site. Similarly, a number of other media sites appear to have been temporarily inaccessible throughout the testing period. The latest OONI measurements show that some previously blocked media websites are now accessible (such as Mada Masr), while other news websites (particularly international ones) remain blocked (such as Al Jazeera).



In an attempt to bypass censorship, some of the blocked media websites have used alternative domains, but this hasn't always been effective. Almesryoon newspaper used the domain elmesryoon.com (instead of almesryoon.com) and recent OONI measurements show that it's accessible (in the one network where it was tested). Daily News Egypt, on the other hand, used thedailynewsegypt.com domain (instead of dailynewsegypt.com), but this alternative domain appears to have been blocked by Egyptian ISPs as well.

To examine the impact of these censorship events, AFTE interviewed staff members working with some of the Egyptian media organizations whose websites were blocked. Lina Atallah, the Editor in Chief of Mada Masr (which was first blocked in May 2017), says:

"We were working normally and suddenly we could not access the Mada site. At the same time, news appeared on pro-regime websites that a group of websites were blocked. Eventually it became clear that the blockpolicy was a systematic policy and not just affecting a group of websites.

We have tried to communicate with various bodies, such as the Journalists Syndicate, the Supreme Council for Media Regulation and the National Telecommunications Regulatory Authority (NTRA), and each party denied its responsibility for the blocking.

Until now, there is no direct contact with any authority or official body. There is no one who declared responsibility for the block. At the same time, we continue to work and use alternative platforms, such as social networks.”

Employees from Masr Al Arabia were also taken aback by the blocking of their site. Editor Adel Sabri says: ***“On 24th May 2017, we suddenly saw this campaign on programs on satellite channels demanding websites to be blocked and a piece of news was published on the site of Al Youm Al Sabee newspaper, saying that 21 websites were blocked, including the site of Masr Al Arabia.”***

“The blocking prevented access for more than 70% of the site’s audience”, says Adel Sabri of Masr Al Arabia. *“This has had an economic impact on our operations,* ***with some companies and banks withdrawing their advertisements from our site. The blocking of our site has also resulted in many sources fearing to deal with our journalists.”*** The latest OONI measurements show that this news website remains blocked in Egypt.

Similarly, the blocking of news website Al Bedaiah had an impact on its audience and on the organization’s operations. Editor in Chief Khalid Al Balashi says: *“Our news website was usually read by several thousands a day. After the block, our team produced content that could not be accessed by the vast majority of our audience, which is quite frustrating in general.”*

But the circumstances surrounding the blocking of Al Bedaiah were different in comparison to those of other Egyptian news organizations.*”I received a call from a colleague working in a newspaper close to the state who told me that there were instructions to attack me. I found an article that insulted me because of an article I did not write,”* said Khalid Al Balashi. ***“When I denied being the author of this article, I received the news from a colleague that the Al Bedaiah site has been blocked.”***

Khaled Al Balashi has since filed a complaint with the Syndicate of Journalists and the Supreme Council of Media Regulation in response to the blocking of the site. He says: ***“After blocking Al Bedaiah, the authorities also blocked the site Masriat, which provides content related to women, moderated by Nefissa***

Elsabbagh. I think the site was only blocked because the Editor in Chief is my wife, since the site is not political."

According to Mada Masr's Lina Attallah, the blocking of media websites can be explained within two contexts:

"The first is the general political context which the authorities are trying to limit, and the second is more specific. It is linked to the internet as a virtual space that allows information circulation. I think there is a set of practices by the authorities to contain the open space provided by the internet, and the blocking of websites is part of it."

Khalid Al Balashi of Al Bedaiah also argues that the blocking of websites is part of a system mentality that does not accept voices that differ from what the authorities say:
"The blocks are in line with current state policies, just as they closed civil society organizations, constrained the workers movement, closed public space and obstructed the media."

Korabia, a news website covering football news locally and internationally, was first blocked in July 2017. According to the site's editors:

"There are more than a hundred journalists, correspondents, and editors who work on the website, and all of them are threatened after we reached a dead end. We entered a dark tunnel again that we don't see an end to, and we do not know who is responsible for these decisions."

A few months ago, Korabia announced on their official Facebook account that they would be suspending their website. The latest OONI measurements show that Korabia's site remains blocked, even though its activities have been suspended.

A month later, blocked news website El Badil also announced that they're not only suspending their website, but also all of their social media platforms and that they will no longer publish any content, whether written or visual. Blocked news outlet Al Bedaiah also suspended its work in recent months, but without an official announcement.

Three lawsuits have been filed in response to the blocking of media websites in Egypt. The first one was filed by Mada Masr, the second was filed by AFTE and the third was filed by the AL-Shurk TV channel. The three lawsuits have been filed before the High Court and sue the Egyptian Ministry of Communications and Information Technology and the National Telecommunications Regulatory Authority. The lawsuits request authorities to explain why their sites were blocked and to disclose which organizations are responsible for the censorship.

On 22nd April 2018, Egypt's High Court rejected Al-Shurk's lawsuit because the channel is not legally registered (and is therefore not authorised to file a lawsuit). Mada Masr's and AFTE's lawsuits are still in process.

Even though Al-Shurk's lawsuit was rejected, the National Telecommunications Regulatory Authority disclosed that their website was blocked following a request from The Committee for Monitoring and Regulating the Muslim Brotherhood Group Funds. The request included seizing entities and funds that belong to the group, as well as banning 16 websites, 16 TV channels and the AL-Masreyoon newspaper.

Human Rights

OONI measurements suggest that human rights websites have been blocked in Egypt as well.

The following table summarizes the amount of network anomalies that each site presented in comparison to the amount of times that it was tested. The high ratio of anomalies, coupled with the accessibility of those sites from global vantage points, suggests that the sites included in the table below were blocked in Egypt.

URLs	Anomalies	Amount of times tested
http://www.sinaihr.org	165	210
http://www.qantara.de	161	186
http://liberties.aljazeera.com/	153	196
http://www.ec-rf.org	152	177
http://www.mom-rsf.org	150	177
http://www.jatoeg.org	137	173
https://www.reporter-ohne-grenzen.de	136	151
https://www.sinaihr.org/	122	159
https://www.hrw.org/	116	176
http://www.anhri.net	86	212

The Sinai Organization for Human Rights is an NGO that monitors and documents human rights violations in the Egyptian Sinai region. The blocking of their site may be politically motivated, given the ongoing conflict in the Sinai peninsula between Islamist militants and Egyptian security forces.

Other blocked human rights websites include the Arabic Network for Human Rights Information, Human Rights Watch, Reporters without Borders, the Egyptian Commission for Rights and Freedoms and the Journalists Observatory against Torture. The blocking of Human Rights Watch appears to have started by 1st October 2017, possibly motivated by the publication of a report on torture in Egyptian prisons.

Mohamed Lotfi, the Executive Director of the Egyptian Commission for Rights and Freedoms (ECRF), says:
"Our website was blocked on the morning of 5th September 2017. We had just launched a campaign and published a report on the incidents of "enforced disappearance" in Egypt, a few days before the block. We tried to deal promptly with the situation and transferred our content to another unblocked server two weeks after the blocking." According to Lofti: "The authorities have a problem with the circulation of information on the internet and are therefore trying to control it after they have already taken control of traditional media and newspapers. I do not think the authority will succeed in that."

Political Criticism

Various websites and blogs that express political ideas were found to be blocked throughout the testing period. The following table summarizes the amount of network anomalies that each site presented in comparison to the amount of times that it was tested.

URLs	Anomalies	Amount of times tested
http://baheyya.blogspot.com	152	212
http://www.manalaa.net	138	207
http://medium.com	86	184
http://ikhwanonline.com/	355	426
http://6april.org	172	205
http://fakartany.com	167	197
http://www.ikhwanonline.com/new/Default.aspx	161	207
http://www.gwady.net	160	198
http://revsoc.me	158	206

One of Egypt's *first* blogs - *the blog of Manal and Alaa* - was amongst the blocked sites. This blog has supported blogging activities since its inception in 2004, hosting other Egyptian blogs and providing technical support when blogging started in Egypt. Another blog offering commentary and analysis of Egyptian politics was amongst those found to be blocked, along with popular blogging platform medium.com and a website discussing a variety of Egyptian political issues.

In 2008, the April 6 Youth Movement sprung as an Egyptian activist group in support of workers who were planning to strike on 6th April. This group has sparked dynamic debates in Egypt, but an Egyptian court banned their activities four years ago. Their site was amongst those found to be blocked, along with another website that shares socialist content.

Think tank fakartany.com appears to be blocked with the usual IP-based rule at approximately the same network location where Deep Packet Inspection (DPI) devices where identified (based on testing from our Raspberry Pi deployments in Egypt). Unlike the other sites, however, it does not trigger RST injection, but packets are just dropped. This may make sense from an engineering standpoint, to put less load on DPI devices, or to block a service at that IP that is not "ordinary" HTTP/HTTPS. This case highlights some variance in terms of the different network filtering rules carried out by Egyptian ISPs.

Circumvention Tool Sites

A number of web proxies and circumvention tool sites were found to be blocked, making censorship circumvention harder in Egypt. The findings are summarized in the following table.

URLs	Anomalies	Amount of times tested
http://www.http-tunnel.com	187	393
https://ooni.torproject.org	168	184
https://explorer.ooni.torproject.org	168	190
http://www.hsselite.com	165	199
https://bridges.torproject.org	163	188
https://www.torproject.org	150	166
https://www.hotspotshield.com/	148	179
http://www.hotspotshield.com	147	179
https://www.thehiddenwiki.org	134	161
http://www.anonymsurfen.com	132	398
http://anonymizer.secuser.com	127	420

https://www.hotspotshield.com	121	162
http://www.zensur.freerk.com	119	382
http://www.xroxy.com	109	385
http://www.jmarshall.com/tools/cgiproxy/	107	387
http://www.suedeproxy.info	106	177
http://www.inetprivacy.com	106	397
http://www.ultimate-anonymity.com	104	380
http://www.stupidcensorship.com	101	385
http://www.webproxyfree.net	93	177
http://www.saoudiproxy.info	92	178
https://psiphon.ca/	86	189
https://www.anonymizer.com/	83	178
https://psiphon.ca	80	143
https://freenetproject.org/	79	190
http://www.vpnbook.com	76	178
http://www.unblockweb.co	76	165
http://www.proxy-list.org	76	187
http://www.hola.org	75	187
http://www.ninjaweb.xyz	75	163
http://www.anonymizer.com	74	166
http://www.unblockfreeproxy.com	72	165
http://www.orangeproxy.net	72	165
http://www.hidester.com	71	159
http://www.unblockytproxy.com	71	187
http://www.dolopo.net	71	182
http://www.freeproxyserver.co	71	162
http://www.northghost.com	71	174
http://www.cactusvpn.com	71	162

Many other circumvention tool sites also presented network anomalies as part of the testing, but we have limited the findings to those that presented the highest ratio of anomalies in comparison to the amount of times that they were tested throughout this study.

Popular censorship circumvention tools are among the blocked sites, such as torproject.org, hotspotshield.com and psiphon.ca. Subdomains of torproject.org - such as bridges.torproject.org and ooni.torproject.org - were blocked as well. Egyptian ISPs don't appear to limit their blocking to censorship circumvention tool sites, since they also appear to block access to the Tor network as well.

Blocking of Tor

The Tor network offers online anonymity, privacy and censorship circumvention, and has therefore become a target of censorship by several governments around the world. In such countries, users can circumvent the blocking and connect to the Tor network through the use of Tor bridges. As part of this study, we analyzed network measurements collected from Egypt through the use of OONI's Vanilla Tor and Bridge Reachability tests, which are designed to measure the blocking of the Tor network and the default bridges part of Tor Browser.

Most of the recent Vanilla Tor measurements have primarily been collected from two networks: Link Egypt (AS24863) and Telecom Egypt (AS8452). These measurements suggest that the Tor network is inaccessible, since the tests weren't able to bootstrap connections to the Tor network within 300 seconds. In recent months, more than 460 measurements collected from these networks show connections to the Tor network consistently failing, strongly suggesting that access to it is blocked. Similarly, measurements collected from Etisalat Misr (AS36992), Mobinil (AS37069) and Vodafone (AS36935) indicate that access to the Tor network is blocked, since many attempted connections have been unsuccessful over the last year and a half. The Tor bootstrap process is likely being disrupted via the blocking of requests to directory authorities.

Few bridge reachability measurements have been collected from Egypt, limiting our ability to examine their potential blocking more extensively over time and across networks. These measurements were collected in June 2017 from the Telecom Egypt (AS8452) and Vodafone (AS36935) networks. Vodafone appears to be blocking obfs4 (shipped as part of Tor Browser), since all attempted connections were unsuccessful (though it remains unclear if *private* bridges work). All measurements collected from Telecom Egypt show that obfs4 works.

Defense in Depth Strategy for Network Filtering

Security experts are probably familiar with the "defense in depth" concept in which multiple layers of security controls (defense) are placed throughout an IT system. The "defense in depth" approach generally aims to provide redundancy in the event that a security control fails or a vulnerability is exploited.

Network measurement testing conducted via Raspberry Pis deployed in Egypt suggests that ISPs appear to be applying a "defense in depth" strategy for networking filtering, particularly in relation to the blocking of fj-p.com: the site of Egypt's Freedom and Justice Party (FJP).

When accessing http://www.fj-p.com, a user is redirected to http://fj-p.com which is served from an unknown location via a CloudFlare CDN. Both http://www.fj-p.com and http://fj-p.com are blocked, but they appear to be blocked by *different* firewall implementations.

We have previously identified a middlebox in Egypt, fingerprinted with IPID 0x1234. Our latest testing, though, shows that there is also another middlebox, fingerprinted with IPID 0x0000. Both middleboxes are located within the same Egyptian network, but the latency to those middleboxes is slightly different: 0x1234 is ~33ms away, while 0x0000 is closer at ~30ms away.

The following traceroute does not explicitly highlight the exact IP addresses of the middleboxes, but helps to understand the possible route of the “censored” HTTP request through the network.

```
HOST: lepidopter             Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???   10.x.y.z         0.0%    10    0.6   0.6   0.6   0.7   0.0
  2. AS???   10.x.a.b         0.0%    10    1.0   0.9   0.9   1.0   0.0
  3. AS???   ???            100.0%    10    0.0   0.0   0.0   0.0   0.0
  4. AS20928 bng.rams.ca (217.139.253.19)
                             0.0%    10   38.8  33.9  29.7  38.8   3.1
  5. AS???   172.17.51.73     0.0%    10  116.5  44.1  32.4 116.5  25.6
  6. AS2914  185.84.18.93     0.0%    10   65.8  66.5  63.6  70.1   1.7
```

When comparing these two middleboxes, 0x1234 does *not* set DF (Don’t fragment) field of the IP header of TCP RST packet, but 0x0000 does. The 0x1234 middlebox *seems* to have an initial IP TTL of 64 (the client sees 59), while 0x0000 has an IP TTL of 32 (the client sees 28). 64 and 32 are assumptions based on the fact that TTL values are usually aligned with the power of 2. Hop distance is well-aligned with extra latency (0x1234 ~ 5 hops ~ 33ms, 0x0000 ~ 4 hops ~ 30ms).

The *raw* TCP window size value is also static and different between the two middleboxes. 0x1234 has a raw window size value of 32120, while 0x0000 is 229. The window size value does not matter for RST packet, but it’s a mandatory field of TCP header.

The 0x1234 RST packet has no payload, while the 0x0000 RST packet has 22 zero-bytes (that's not "Ethernet padding", but real zero bytes according to the length field of IP packets). Moreover, sending those two HTTP requests to a random IP address (e.g. one of Google's IPs: 216.58.206.14) also triggers two different firewalls/middleboxes having a slightly different configuration. The experiment of sending two unrelated HTTP requests to a single Google IP address is done to ensure that these two middleboxes interpreting the HTTP protocol are on the same network path from the client's IP to the server's IP, and that that's not just two distinct middleboxes on two distinct paths.

All of the above suggests that there are two different middleboxes doing the filtering on that specific path, triggered by slightly different rules: a request to http://www.fj-p.com triggers the 0x0000 middlebox, while a request to http://fj-p.com triggers the 0x1234 middlebox.

This appears to be a "defense in depth" strategy applied to censorship, confirmed by doing a TCP traceroute with HTTP payload. A request to http://www.fj-p.com (that triggers the 0x0000 middlebox that is closer) receives RST since the client's TTL=5, while http://fj-p.com (that triggers the 0x1234 middlebox, is ~3..4ms further away, and that has a *hypothetical* reverse-path of one hop longer) receives RST since the TTL=6 (as confirmed by a small series of experiments).

Moreover, the 0x0000 middlebox does not appear to be able to reassemble HTTP requests in some cases. Some extra testing with http://www.fj-p.com shows that when the HTTP verb (e.g. `GET`) is split in the middle (like `GE || T ...`), there is no *usual* RST at TTL=5 from 0x0000, but there is RST with TTL=6 from 0x1234. This strongly suggests that these two middleboxes behave differently when the HTTP verb is split.

Both middleboxes, however, appear to reassemble split `Host` headers. When splitting the domain in the middle, `Host: www.f || j-p.com` triggered the 0x0000 middlebox, while `Host: fj-p. || com` triggered the 0x1234 middlebox (as expected).

In short, both middleboxes replaced the original requests with RST packets when forwarding them to servers (since the TTL field set by the client was preserved while forwarding the packet). This suggests that both middleboxes are "in-path" (man-in-the-middle), not "on-path" (man-on-the-side), leading us to think that Egyptian ISPs are applying "defense in depth" tactics for network filtering.

Interference of SSL Traffic towards the Cloudflare CDN

The traffic between Cloudflare's Point-of-Presence in Cairo and the backend servers of sites using Cloudflare (which are located *outside* of Egypt) appears to be *filtered*.

Hundreds of OONI Probe network measurements presented Cloudflare-specific errors (such as 525, which occurs when the SSL handshakes to Cloudflare fails), suggesting that Egyptian ISPs are blocking sites that use Cloudflare by interfering with SSL encrypted traffic between the Cloudflare CDN and the website backend.

We excluded unencrypted HTTP sites that presented such anomalies (such as zenvpn.net and tunnelbear.com) in case the channel between the client and Cloudflare was tampered with, and limited our findings to encrypted HTTPS sites (enabling us to confirm their blocking with more confidence). This left us with circumvention tool sites psiphon.ca and purevpn.com, and news website ultrasawt.com, which appear to be blocked by some form of network interference on the SSL connection between the websites' backend servers and a Cloudflare CDN in Egypt.

This particular type of network interference could either be attributed to a man-in-the-middle attack on the SSL encrypted connection between Cloudflare and the website backend (as suggested by data from other tests), or to a man-on-the-side attack to terminate or interfere with the SSL handshake.

All of the measurements pertaining to these cases are available **here**.

Ad Campaign

Network anomalies reported in Egypt in 2016 sparked an investigation by OONI, leading to the publication of a research report that unveiled the covert presence of what appears to be an ad campaign.

OONI's investigation found that at least one ISP, state-owned Telecom Egypt (TE), was using Deep Packet Inspection (DPI) technology to conduct man-in-the-middle attacks to redirect users (attempting to access certain sites, such as pornography) to affiliate ads or malware.

A few months ago, the Citizen Lab published a research report which built upon OONI's investigation, uncovering the breadth and scale of Egypt's use of DPI devices to covertly raise money through affiliate ads and cryptocurrency mining.

More specifically, they found that the ad injection identified by OONI in 2016 was probably the result of Sandvine PacketLogic devices and that (at least) 17 Egyptian ISPs carried out such injections. They also found that ISPs redirected users' unencrypted HTTP connections to browser cryptocurrency mining scripts, in addition to revenue-generating content, such as affiliate ads.

Our analysis of all OONI Probe network measurements collected from Egypt over the last year includes hundreds of measurements (collected from multiple ASNs) that show the redirection of unencrypted HTTP connections to affiliate ads and cryptocurrency mining scripts, suggesting the presence of an ad campaign.

Egyptian ISPs don't seem to have a common policy in terms of how they implement redirects over time. In some cases, they appear to be implementing a chain of HTTP redirects, while in other cases, they implemented intermediate javascript-based redirects (which were sometimes obfuscated). And in some other cases, the redirects appear to be served directly from their DPI equipment.

The following table summarizes the amount of redirects that we found per ASN in each month between June 2017 to March 2018 (after which we found *no* other redirects in OONI measurements). We also provide a sample of *some* of the affected URLs and redirects per month, and list the total amount of measurements presenting redirects per ASN.

Date	Affected ASNs & Redirect Count	Sample of Affected URLs	Traffic Sinks
2017-06	28 — LINKdotNET, 23 — TE Data, 4 — Etisalat	islamic-relief.org, wilpf.org, 4genderjustice.org and 31 more.	go.pub2srv[.]com, vidz4fun[.]com (via ceesty.com), rapidyl[.]net
2017-07	23 — TE Data, 13 — LINKdotNET, 1 — Noor	2 "dead" websites	rapidyl[.]net
2017-08	54 — TE Data, 15 — LINKdotNET, 2 — Noor	garem.org, ppsmo.org, and 9 more	rapidyl[.]net
2017-09	30 — TE Data, 7 — LINKdotNET, 1 — Noor	anpbolivia.com, crazyshit.com, ppsmo.org, and 4 more	rapidyl[.]net
2017-10	32 — TE Data	ppsmo.org and 2 more	rapidyl[.]net
2017-11	29 — TE Data, 6 — LINKdotNET, 3 — Vodafone	2 "dead" websites	hitcpm[.]com (via vidz4fun), rapidyl[.]net, hitcpm[.]com
2017-12	60 — TE Data, 7 — LINKdotNET, 3 — Noor	euthanasia.cc, sakhr.com, womeninblack.org, stshenouda.com and 34 more	infads-1372369412.eu-west-1.elb.amazonaws[.]com, ylx-4.com, hitcpm[.]com
2018-01	3 — Vodafone, 2 — TE Data, 1 — LINKdotNET, 1 — Noor	89.com, likud.org.il, and 4 more	infads-1372369412.eu-west-1.elb.amazonaws[.]com, ylx-4.com
2018-02	3 — LINKdotNET, 2 — TE Data	bglad.com, guerrillagirls.com, and 2 more	conceau[.]co, ylx-4[.]com (new ID)
2018-03	2 — TE Data, 1 — LINKdotNET	bglad.com and one more	ylx-4[.]com

From the above table, it's evident that (at least) five Egyptian ISPs carried out an ad campaign between June 2017 to March 2018: Link Egypt, Telecom Egypt, Etisalat Misr, Noor, and Vodafone. Based on OONI measurements, these ISPs redirected unencrypted HTTP connections to content hosting affiliate ads.

The above table includes *some* of the affected URLs per month, including: the Palestinian Prisoner Society, the Women's International League for Peace and Freedom, the Women's Initiatives for Gender Justice and Women in Black.

Detailed information based on our analysis, showing *all* of the affected sites and the injected redirects, is available **here**. A wide range of *different types of sites* were affected, including news websites, human rights sites, LGBTQI sites, VPN sites, Israeli sites, and porn sites. Egyptian ISPs even appear to redirect users attempting to access websites of the United Nations, such as un.org and ohchr.org.

Interestingly enough, we have not found any redirects or traces of an ad campaign after 9th March 2018, which coincides with the publication of the Citizen Lab's research report on the issue. That said, it remains unclear if the ad campaign has terminated or not, particularly since the lack of redirects in recent measurements could potentially be attributed to a number of factors.

The above table, for example, shows that different URLs have been affected over time, and that redirects were only served for some URLs for a few months. We therefore cannot exclude the possibility of redirects being served for *other* URLs that weren't tested over the last few months.

Our findings are limited by the amount and types of URLs that were tested during this study, as well as by the URL selection bias (see the Methodology and Acknowledgement of Limitations sections of this report).

It's worth highlighting that *not* all of the redirects that we found in OONI Probe measurements are malicious or for profit. Egyptian ISPs also injected notifications to inform users that they're using outdated browsers (without proposing a specific browser, but redirecting to https://browsehappy.com/) and to remind them to top up their accounts.

Localizing Middleboxes

Over the last year, localizing middleboxes used as part of ad campaigns in Egypt has become more challenging. In 2016, OONI reported that their latency analysis showed that Deep Packet Inspection (DPI) equipment sent redirects *before* a website sent its HTTP response, without terminating the session to the server (hence sending `408 Request Timeout` errors). This helped refute the hypothesis of sites potentially being infected with malware as part of redirects to malicious content.

The Citizen Lab's recent report, however, shows that the redirects were injected upon receipt of an HTTP response, rather than an HTTP request. This suggests that Egyptian ISPs may have changed their DPI equipment over the last year and a half, raising the question of whether it has potentially been tuned to avoid latency-based detection.

Given that we haven't found redirects in recent OONI measurements post March 2018 (as mentioned in the previous section), our ability to examine this further has been limited.

Conclusion

Over the last year, internet censorship in Egypt appears to have become more dynamic, sophisticated and pervasive.

More than 1,000 URLs presented network anomalies throughout the testing period, 178 of which consistently presented a high ratio of HTTP failures, strongly suggesting that they were blocked. Rather than serving block pages, Egyptian ISPs appear to primarily block sites through the use of Deep Packet Inspection (DPI) technology that resets connections. Both HTTP and HTTPS sites appear to have been blocked.

In some cases, instead of RST injection, ISPs appear to drop packets, suggesting a variance in filtering rules. In other cases, ISPs appear to be interfering with the SSL encrypted traffic between Cloudflare's Point-of-Presence in Cairo and the backend servers of websites hosted outside of Egypt. Latency measurements over the last year and a half also suggest that Egyptian ISPs may have changed their filtering equipment, making the latency-based detection of middleboxes more challenging.

More than 100 URLs that belong to media organizations appear to have been blocked, even though Egyptian authorities only ordered the blocking of 21 news websites last year. These include Egyptian news outlets (such as Mada Masr, Almesryoon, Masr Al Arabia and Daily News Egypt), as well as international media sites (such as Al Jazeera and Huffington Post Arabic). In an attempt to circumvent censorship, some Egyptian media organizations set up alternative domains, but (in a few cases) they got blocked as well.

Through interviews, staff members of blocked Egyptian media websites reported that the censorship has had a severe impact on their work. In addition to not being able to publish and losing part of their audience, the censorship has also had a financial impact on their operations and deterred sources from reaching out to their journalists. A number of Egyptian media organizations have suspended their work entirely, as a result of persisting internet censorship.

Many other websites, beyond media, appear to have been blocked as well. These include human rights websites (such as Human Rights Watch, Reporters without Borders, the Arabic Network for Human Rights Information, the Egyptian Commission for Rights and Freedoms, and the Journalists Observatory against Torture) and sites expressing political criticism (such as the April 6 Youth Movement), raising the question of whether censorship decisions were politically motivated.

Egyptian ISPs appear to be applying "defense in depth" tactics for network filtering by creating multiple layers of censorship that make circumvention harder. This is in part suggested by the blocking of numerous censorship circumvention tool sites (such as torproject.org, hotspotshield.com and psiphon.ca), as well as by the widespread blocking of the Tor network. In some cases, Tor bridges appear to be blocked as well.

What stands out though as a "defense in depth" strategy is the blocking of Egypt's Freedom and Justice Party (FJP) site. Our testing shows that different versions of this site (http://www.fj-p.com and http://fj-p.com) were blocked by *two* different middleboxes. In doing so, Egyptian ISPs added extra layers of censorship, ensuring that circumvention requires extra effort.

While the legal justification behind the blocking of all of these websites remains quite unclear, it can probably be attributed to a number of Egyptian laws, such as Article 3 of the Emergency Law, Article 29 of the Anti-Terrorism Law, or Article 7 of the recently approved Cyber Crime Law.

This is also suggested by the May 2017 order which banned certain media websites on the grounds of "supporting terrorism and lies", in reference to such laws.

Furthermore, the National Telecommunications Regulatory Authority disclosed that Al-Shurk TV channel's website was blocked following a request from The Committee for Monitoring and Regulating the Muslim Brotherhood Group Funds. This request also included bans for a number of other media websites.

Apart from censorship, Egyptian ISPs appear to be carrying out an ad campaign as well. Hundreds of OONI Probe network measurements (collected from multiple ASNs) show the redirection of unencrypted HTTP connections to affiliate ads and cryptocurrency mining scripts. Egyptian ISPs appear to be using DPI (or similar networking equipment) to hijack unencrypted connections and inject redirects, though they don't seem to have a common policy in terms of how they implement these redirects over time.

A wide range of different types of URLs were affected, including the Palestinian Prisoner Society, the Women's Initiatives for Gender Justice, LGBTQI sites, VPN sites, Israeli sites, and even websites of the United Nations, such as un.org and ohchr.org.

While certain Egyptian laws may justify the censorship events identified as part of this study, the extent to which an ad campaign is justifiable remains unclear. The aim of this study was to examine censorship events through the analysis of network measurements, supporting future research efforts and public debate.

Acknowledgements

We thank all the volunteers in Egypt who have run and continue to run OONI Probe, thus making this research possible.

We also thank the translators of this report, Elio Qoshi for the design of its PDF document, Arturo Filasto and our Egyptian friends for review and support.