

Measuring Internet Censorship in Cuba's ParkNets



Image by Arturo Filastò (CC-BY-SA-3.0)

A research study by the Open Observatory of Network Interference (OONI)

28th August 2017

Table of contents

[Key Findings](#)

[Introduction](#)

[Background](#)

[Network landscape and internet penetration](#)

[ETECSA](#)

[ParkNets](#)

[Joven Club](#)

[StreetNets](#)

[El Paquete](#)

[Summary](#)

[Measuring internet censorship in Cuba](#)

[Methodology](#)

[Collection and analysis of ooniprobe network measurements](#)

[Custom tests](#)

[Findings](#)

[Blocked websites](#)

[News Media](#)

[Political Criticism](#)

[Human Rights Issues](#)

[Anonymity and Circumvention Tools](#)

[Communication Tools](#)

[Culture](#)

[Religion](#)

[Militant](#)

[Skype blocked](#)

[Deep Packet Inspection \(DPI\) technology](#)

[Huawei equipment in Cuba](#)

[Google App Engine blocked by Google](#)

[Acknowledgement of limitations](#)

[Conclusion](#)

Authors: Maria Xynou, Arturo Filastò, Simone Basso

OONI tests: [Web Connectivity](#), [HTTP Host](#), [HTTP Header Field Manipulation](#), [HTTP Invalid Request Line](#), [Vanilla Tor](#), [Meek Fronted Requests](#), [Facebook Messenger test](#), [WhatsApp test](#), [Telegram test](#), [Network Diagnostic Test \(NDT\)](#)

Probed ISP: ETECSA (AS27725)

Testing period: 29th May 2017 to 10th June 2017

Censorship method: Deep Packet Inspection (DPI) technology serving blockpages and RST Injection

Key Findings

[OONI network measurement data](#), collected from eight vantage points across three Cuban cities between 29th May 2017 to 10th June 2017, confirms the **blocking of 41 websites**. Deep Packet Inspection (DPI) technology, which we suspect to be located in Havana, was used to reset connections to those sites and serve (blank) block pages. Only the HTTP version of those sites was blocked, potentially enabling users to circumvent the censorship by merely accessing them over HTTPS.

Most of the blocked sites have one main thing in common: they *express criticism* towards the Castro regime, directly or indirectly.

The blocked sites include:

- News outlets and blogs expressing political criticism and covering human rights issues in Cuba;
- The [independent news outlet](#) created by [Yoani Sanchez](#), a prominent Cuban blogger;
- The [Cuban Free Press Project](#) which [aims](#) to support journalists and independent writers;
- A [Cuban online forum](#);
- Pro-democracy sites;
- [Freedom House](#), which [publishes](#) annual reports on press freedom and net freedom;

- [“Ladies in White”](#): Peaceful opposition [movement](#) led by the wives and female relatives of jailed dissidents;
- [Cuba Sindical](#), which promotes [independent trade unions](#);
- [Anonymouse](#), amongst other web proxies;
- Anti-Castro groups: [Alpha 66](#) and [“Brothers to the Rescue”](#).

Interestingly enough though, various other international sites which also express criticism - such as Reporters Without Borders’ [portrait of Cuba’s President](#), presenting him as a “Predator of Press Freedom” - were found to be [accessible](#) across Cuba. This might indicate a lack in sophistication in both internet surveillance and censorship.

Skype was the only popular communication tool that we found to be blocked.

Other popular platforms, like [Facebook Messenger](#) and [WhatsApp](#), were accessible across Cuba. While some web proxies were found to be blocked, the [Tor network](#) was [accessible](#) during the testing period of this study.

Chinese vendor Huawei was found to be supporting Cuba’s internet infrastructure. While it is clear that Cuba is using Huawei’s access points, it remains unclear whether and to what extent Huawei equipment is actually being used to implement internet censorship in the country.

It was clear though that Google was blocking IP addresses originating from Cuba from accessing Google App Engine, at least during the testing period of this study.

The [high cost of the internet](#) (especially in comparison to [local salaries](#)) and the [limited availability of wifi hotspots](#) across Cuba remain the main barriers to accessing the internet.

Introduction

Last May, the [OONI](#) team visited Cuba. We ran a variety of network measurement tests across eight vantage points in Havana, Santa Clara, and Santiago de Cuba, with the aim of measuring internet censorship.

We obviously ran our own network measurement software, [ooniprobe](#), which is designed to [examine various forms of internet censorship](#). We also ran other network tests, particularly in response to ooniprobe findings, such as latency measurements to blocked sites, traceroutes, and network scans.

This research report documents our key findings from the network measurement tests that we performed in Cuba. The aim of this study is to increase the research community's understanding of information controls in Cuba based on [empirical data](#).

The following sections of this report provide information about Cuba's network landscape and internet penetration levels. The remainder of the report documents the methodology and findings of this research study.

Background



Image by Arturo Filastò (CC-BY-SA-3.0)

The Republic of Cuba is a Central American archipelago of islands located in the northern Caribbean sea. Its population is multi-ethnic with European, African, and Native American ancestry, and consists of [around 11 million](#). The vast majority of Cuba's population is Roman Catholic ([85%](#)) as a result of Spanish colonization between the 15th and 19th centuries.

Following the Spanish-American war, Cuba gained formal independence and the Republic of Cuba was [established in May 1902](#). Fulgencio Batista served as Cuba's

President between 1940 to 1944, during which he instated Cuba's 1940 Constitution, which was [considered progressive](#) for its time. In 1952 though he [staged a coup with U.S. support](#), outlawing the Cuban Communist Party, suspending the 1940 Constitution, and revoking most political liberties. High unemployment and general political dissatisfaction throughout the 1950s resulted in various [organizations competing for public support to bring about political change](#). The Cuban Revolution began in 1953, led by Fidel Castro's 26th July Movement and its allies, overthrowing Batista's dictatorship and forcing him into exile on 1st January 1959.

Castro [legalized the Communist Party and promulgated the Agrarian Reform Law](#). Through a series of laws relating to land reform, passed between 1959 to 1963, thousands of acres of farmland were expropriated, including those of large U.S. landholders. The nationalization of U.S.-citizen-held property deteriorated the relationship between Cuba and the U.S., resulting in a range of sanctions in the early 1960s, including a total ban on trade between the two countries. Cuba then established [economic relations with the Soviet Union](#), depending on it for substantial aid.

Following the collapse of the Soviet Union, Cuba entered a [period of economic crisis](#) (known as the Special Period). As part of measures to cope with the crisis, Cuba allowed some self-employment in certain sectors, legalized the use of the US dollar in business, and encouraged tourism. But as Cuba still has a largely state-controlled planned economy, most of the labor force is employed by the government, and most means of production are run and owned by the government. Cubans are entitled to a [monthly supply of food](#) and other staples, but the average monthly wage is only around US\$20.

Cuba is now one of the world's last remaining socialist countries following the Marxist-Leninist ideology. Following [decades of U.S embargo against Cuba](#), the two governments reached a deal in July 2015 to reopen embassies in their respective capitals and to [re-establish diplomatic relations](#). President Trump though has recently [reversed some actions taken by the Obama administration](#).

Network landscape and internet penetration

Cuba is one of the countries in the world with the most [restricted internet](#).

Even though the internet was first introduced in Cuba in the late 1990s, internet access has been limited by various factors. Cuban [government policies restricted access](#) to the internet, as the telecommunications sector was viewed as a [tool for the subversion](#) of

the country's political system. Following the fall of the Soviet Union, Cuba had a major [economic crisis](#), limiting the availability of funds that could support internet infrastructure. Meanwhile, the [U.S. trade embargo](#) made internet equipment expensive and difficult to obtain. The Cuban government also feared that foreign investment could undermine national sovereignty.

Up until 2008, private ownership of a computer or cell phone [required a government permit](#) that was difficult to obtain. But over the last few years, Cuba's internet landscape has gradually been changing. In December 2014, Presidents Barack Obama and Raul Castro reached an [agreement to restore diplomatic relations](#). Earlier that year, Google's executives [visited Cuba](#) to initiate discussions. In April 2017, Google became the [first foreign internet company to launch its servers in Cuba](#).

Yet, only [32.5%](#) of Cuba's population has access to the internet. The sections below provide an overview of Cuba's unique internet landscape.

ETECSA



Image by Arturo Filastò (CC-BY-SA-3.0)

As of 2013, Cubans can sign up with [Empresa de Telecomunicaciones de Cuba S.A. \(ETECSA\)](#), the country's *only* telecom company, which is state-owned.

To connect to the internet, Cubans need to purchase a [temporary or permanent account](#) from ETECSA. Temporary accounts are most commonly used by tourists, particularly since permanent accounts are primarily provided to Cuban residents. A temporary account is valid for 30 days, while a permanent account is valid for 360 days (from the first connection to the internet).

A temporary account is provided in the form of a card, which includes a login code and a password, both of which are long strings of numbers. ETECSA cards offer 30 minutes, 1 hour, or up to 5 hours of internet access. Once connected to a wifi, browsers present the Nauta captive portal, which is where users are required to enter the login code and password from their ETECSA cards.

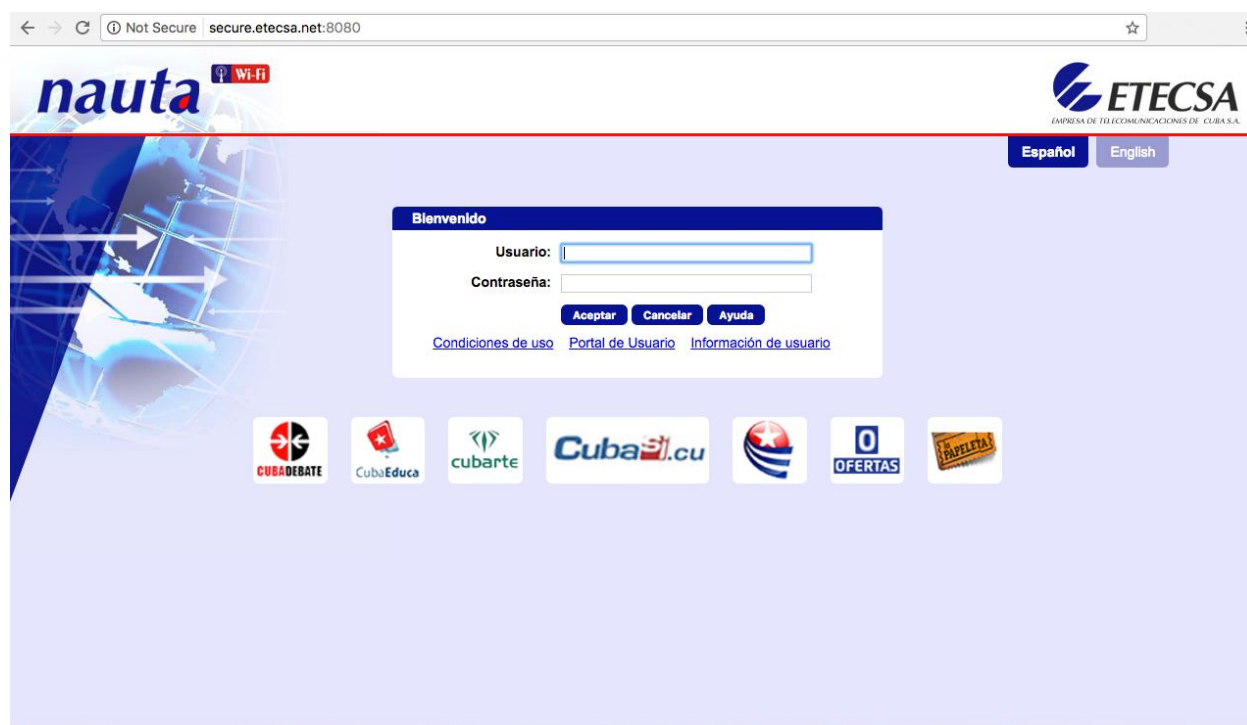


Image: Nauta captive portal

It's worth noting that unless users have deleted all of their browser cookies, they are unable to login via the Nauta portal. This in itself could potentially be viewed as a barrier to accessing the internet for users who don't know how to delete their browser cookies (or who aren't aware that they should be doing so).

Permanent accounts don't require ETECSA cards. Rather, Cubans are issued usernames and passwords when they purchase permanent accounts from ETECSA, which they can charge and recharge for up to a year at a time. Interestingly enough, Cubans can top up their permanent accounts to solely gain [access to the national web \(intranet\) at 0.10 CUC per hour](#), while accessing the international web (internet) is more than ten times more expensive, at [1.5 CUC per hour](#). This separation of the national and international web is not provided as an option for temporary accounts, perhaps because it is assumed that they are mostly used by tourists. In addition to internet and/or intranet access, permanent accounts also provide Cubans with an @nauta.cu email address.

nauta

Servicio público de acceso a Internet

-Navegación internacional **1.50 CUC / hora**

-Navegación nacional **10 centavos CUC / hora**

CUENTAS

Temporales
Tarjetas prepagadas válidas por **30 días** luego de su primera utilización.

Permanentes
Válidas por **360 días**.

Modalidades de servicios:

- Cuenta de navegación internacional con cuenta de correo @nauta.cu
- Cuenta de navegación nacional

¡NAVEGA POR MI CUBA!

Recargables mediante:

- Recargas internacionales
- Recarga mínima directa: 0.10 CUC
- Cupones

Recarga nauta Recarga nauta Recarga nauta Recarga nauta

Para más información **Contáctenos...** **118** www.etecsa.cu

ETECSA
EMPRESA DE REGULACIÓN DE COMUNICACIONES DE CUBA S.A.

Source: ETECSA, http://www.etecsa.cu/internet_conectividad/internet/

When we visited ETECSA offices in Cuba to purchase temporary accounts, we were requested to provide our passports. Similarly, all other tourists and residents appeared to be providing their IDs when purchasing accounts. ETECSA employees though didn't appear to be linking our IDs to the specific accounts that we were issued. Rather, it seemed that identification was requested merely to track how many ETECSA cards

were issued per person. In total, we could only buy up to three cards each. This might be a strategy in an attempt to limit the reselling of ETECSA internet cards.

While accounts should officially be purchased from the ETECSA offices, many temporary accounts are resold on the streets at higher prices. Some Cubans stock up on ETECSA cards and sell them at twice the price on the streets, usually around public wifi hotspots. When purchased from an ETECSA office, [temporary accounts cost 1.5 CUC for 1 hour of internet access](#). Re-sellers, on the other hand, often sell the same temporary ETECSA cards for 3 CUC. Given that ETECSA offices often have long queues (and may not always be close to public wifi hotspots), many (particularly tourists) resort to buying the more expensive ETECSA cards sold on the streets.

The table below illustrates the cost of internet access, depending on the type of account (temporary or permanent) and the amount of time used.

Tipo de cuenta	Servicio	Tarifa	Ciclo de vida de la cuenta
Temporal	Tarjetas de 30 minutos	0.75 CUC	30 días a partir de la primera conexión
	Tarjetas de 1 hora	1.50 CUC/hora	
	Tarjetas de 5 horas	7.50 CUC	
Permanente	Navegación internacional con cuenta de correo internacional	1.50 CUC/hora	330 días activa y 30 días no activa, válidos solo para recargar
	Navegación nacional	0.10 CUC/hora	

Source: ETECSA, http://www.etecsa.cu/internet_conectividad/internet/

On average, Cubans [earn around 25 CUC](#) per month. Since only 1 hour of internet use [costs 1.5 CUC](#) (if bought from the official ETECSA offices, otherwise it may be more expensive), it's likely that most Cubans restrict their use to the country's national intranet, which is far more affordable. Given the high cost of accessing the internet (especially in comparison to local salaries), it's probably no surprise that only [32.5%](#) of Cuba's population currently has access to the internet.

ETECSA provides [ADSL services](#) for the commercial and state sector. Given that only 1 Mbps costs 16,000 CUC per year, it's clear that ADSL services are currently out of reach for most Cubans. ETECSA also offers [point-to-point connections](#) to businesses at

a fixed monthly rate. According to ETECSA, full-time connection is guaranteed with a maximum transmission speed of up to 2 Mbps. Similarly, ETECSA enables businesses to access and use the internet via [ATM and Ethernet](#). All such services, however, cannot be used by the Cuban public, mainly due to their high cost.

Previously, Cubans could only access the internet via [computer centres](#) across the country. Many of these centres are called “[Joven Club](#)” and they provide computer classes (including programming courses) to young Cubans. In 2015, the Cuban government opened the [first public wifi hotspots](#).

Today, Cubans can [access the internet](#) in ETECSA offices, Joven Clubs, post offices, hotels, airports, and at the public wifi hotspots.

ParkNets



Image by Arturo Filastò (CC-BY-SA-3.0)

Cubans cannot access the internet from the comfort of their homes. Rather, they must visit [public wifi hotspots](#). Cubans therefore have a uniquely different relationship with the internet, in comparison to other countries. They don't access the internet, they *visit* it.

Currently, Cuba has [421 public wifi hotspots](#). The vast majority of these hotspots are located in public parks. Others are located in cafeterias, boulevards, and research centres. One of the wifi hotspots in Santa Clara is, interestingly enough, located right under the Che Guevara Mausoleum. [Most wifi hotspots \(63\) are located in Havana](#), the country's capital. Even though Santiago de Cuba is the country's second largest city, it only has 27 hotspots.

While the amount of hotspots across the country has increased significantly over the last years, some Cuban cities have very few hotspots available. Most of these hotspots are located in parks, which can be too hot and sunny to visit during the day, and too crowded (in some cases) at night (often leading to worse internet speed and performance). The inconvenience of having to visit hotspots, which may not always provide fast and reliable internet, can in itself be viewed as a barrier to accessing the internet in Cuba.

Since [most of the wifi hotspots are located in parks](#), we dubbed them "*ParkNets*". When hanging out in ParkNets, we noticed that almost all Cubans accessed the internet via their mobile phones. We also noticed that they appeared to be using the internet primarily for communications. When talking to locals, they mentioned that - in their view, at least - most Cubans use the internet to connect with their family and friends (many of whom are abroad), and that [Facebook Messenger is extremely popular](#). Given the high cost of accessing the internet, it's probably no wonder why Cubans optimize for using the internet primarily for communications purposes.

Resellers of ETECSA internet cards often lurk in and around ParkNets. But the underground internet business is not restricted to them. We noticed that some locals were using repeaters within ParkNets to sell cheaper internet access to others. In those cases, we noticed that some Cubans were using the internet for purposes that expanded beyond communications, like listening to music or watching viral videos on YouTube.

Joven Club

Cuba has computer centres across the country which provide internet access, computer classes, and even programming courses to the youth. These centres are known as "[Joven Club](#)" ("Youth Club").

While in Cuba, we visited one of these Joven Clubs. To use a computer and gain access to the internet, we were required to provide identification which was most likely linked to our accounts. We were then issued usernames and passwords to use the computers and access the internet. Through these computers, we were able to access both the internet and Cuba's intranet. It's worth emphasizing that the speed of the internet at the Joven Club was incredibly fast, in comparison to that provided at public wifi hotspots.

While browsing Cuba's intranet, we came across [EcuRed](#), which could be viewed as Cuba's version of Wikipedia.

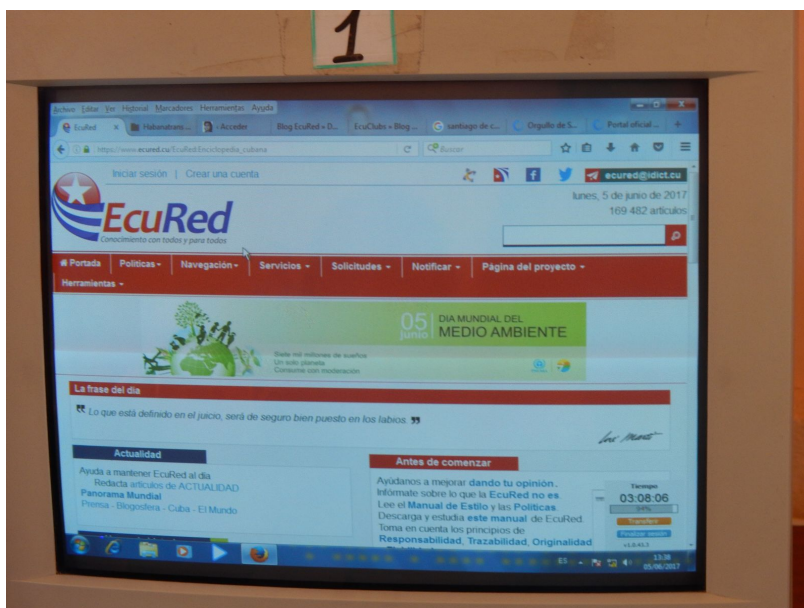


Image: Accessing EcuRed via a computer at Joven Club

EcuRed, created by Cubans and only available in Spanish, serves as an online encyclopedia which aims to “[create and disseminate knowledge from a decolonizing point of view](#)”. Similarly to Wikipedia, EcuRed offers Cubans an interactive space to edit and publish open content. Unlike Wikipedia, EcuRed includes some “protected pages” that can [only be edited by the platform's moderators](#). EcuRed's content falls under a variety of different categories, ranging from art, culture and sports to science, history and politics, as illustrated below.

EcuRed: Categories Tree

Search Categories

Categories Tree

Unused categories

Most Popular Categories

Pressing the plus (+) signs displays the categories tree

Category tree

- ▶ Arts and crafts
- ▶ Applied Sciences and Technologies
- ▶ Medical and Biological Sciences
- ▶ Natural and Exact Sciences
- ▶ Social and Humanistic Sciences
- ▶ Cuba. Organization of the State
- ▶ Culture
- ▶ Sports and Recreation
- ▶ Events
- ▶ People
- ▶ Aeronautical engineering and technology
- ▶ Institutions
- ▶ Regulations
- ▶ Organizations
- ▶ Heritage
- ▶ Awards and Honours
- ▶ Professions

Most Popular Categories

- ▶ Localities of Cuba
- ▶ History of the locality
- ▶ Cuban Revolutionary Martyr
- ▶ Health
- ▶ Plants
- ▶ Animal Biology
- ▶ Historical character
- ▶ Kitchen Recipes
- ▶ Actor
- ▶ Literature
- ▶ Birds
- ▶ Singer
- ▶ Animal behavior
- ▶ Institutions
- ▶ Cinematography

Source: EcuRed, https://www.ecured.cu/index.php/EcuRed:%C3%81rboI_de_Categor%C3%ADas

It's worth noting though that most of its content is written from a Cuban lens.

Recently, EcuRed shared the [100 most read articles](#) on its platform. The top 13 articles include specialized topics, like chemistry, biology and maths, indicating that EcuRed likely has a limited (and specialized) audience.

MAY
30

The hundred of EcuRed (May 2017)

EcuRed inside



We share with our collaborators and followers the list of one hundred articles of EcuRed in the month of May 2017:

Article	Matter	Average time on page (in minutes)
Chemical solution	Chemistry	6.17
Muscular system	biology	6.11
House Rules	Civic	4.29
Communication Barrier	Communication	6.46
Measures of dispersion	Math	6.56
Parallel circuit	electronics	6.16
Work	Physical	7.18
Scientific investigation	Methodology	6.48
Theory of Oparin	biology	6.22
Cubic function	Math	6.22
Endocrine glands	biology	4.48
Plasmatic membrane	biology	7.13
Tables of frequencies	Statistics	5.16











Source: *The hundred of EcuRed (May 2017)*,
<http://ecured.cubava.cu/2017/05/30/los-cien-de-ecured-mayo-de-2017/>

EcuRed also has a [blog](#), which aims to “[provide a space for the free expression of all members of the EcuRed community](#)”, as well as a [social network](#) (called “EquClubs”) for its community of editors.

Other sites on Cuba’s intranet include [CubaEduca](#) and [CubaDebate](#). CubaEduca is the educational portal of Cuba’s Ministry of Education, designed to provide a communication channel for the exchange of information that can facilitate the use of ICTs in education. CubaDebate, on the other hand, is a government-supported news site, edited by the Cuban Journalists’ Association Against Terrorism, which aims to “create a space for the exchange of information on issues related to the subversion and defamatory campaigns organized against Cuba”. CubaDebate ranks as one of the [top sites](#) visited by Cubans.

[Reflejos](#) is another [top-ranking](#) Cuban site which serves as a blog hosting platform. It enables Cubans to publish blogs on a variety of topics. The top blogs that the site recommends include those of the Ministry of Communications and the EcuRed blog, amongst others.






RECOMMENDED BLOGS

	MINCOM Blog		Backpack Blog
	Estanquillo Blog		Ecured Blog
	Sub Committee 7		OUTSIDE
	Cuban Adversary		The guayacán of Cuba
	Run to live		Dota 2 Camaguey

CREATE YOUR BLOG

TO ACCESS

LATEST ENTRIES

-  Enchanting organization of Cuban women and Fidel
-  PLAYMUSIC IS SUFFERING CHANGES
-  OMAR VARELA (DUBSTEP, PIRATE STEP, CUMBIASTEPI)
-  PANDA EYES (DUBSTEP, GLITCH HOP)
-  Hello World!

Source: Reflejos, <http://cubava.cu/> (translated to English)

Two years ago, students and employees at the University of Information Science [launched a digital portal](#) designed to unify all services available on Cuba's intranet. This enables Cubans to browse all images, documents, news articles, and academic papers and blogs published on Cuba's intranet.

Interestingly enough, we didn't come across any blocked sites while browsing the internet via computers in a Joven Club. Most internationally relevant websites were accessible.

Similarly to Joven Clubs, Universities in Cuba require user accounts (linked to IDs) to access the internet. Only University staff and students are authorised to acquire such accounts. Since their online activity is directly linked to their personal accounts, they likely self-censor the types of sites that they access.

StreetNets

Cuba's restrictive internet landscape appears to be fostering *alternative* means of accessing the internet, particularly amongst the youth. As of 2001, a small community of tech-savvy Cubans [started building a mesh network across Havana](#), linking computers to a private network. Today, multiple [mesh networks](#) have sprung across Havana and many other Cuban cities, providing members the opportunity to communicate and share files privately. These networks are known as "[StreetNets](#)", or "SNets" for short.

StreetNets consist of wifi antennas that communicate with each other, or Ethernet cables on rooftops that connect hundreds of computers. StreetNet users play online games, view popular TV shows and movies, communicate, and share files. While StreetNets are technically illegal, especially since the use of wifi equipment requires a license from the Ministry of Communications, [authorities might be turning a blind eye](#). This is likely because users [refrain from discussing politics and/or sharing prohibited materials](#). Self-censorship *might* be the most effective form of censorship in Cuba, even within StreetNets.

El Paquete



Image by Arturo Filastò (CC-BY-SA-3.0)

Cuba's underground internet is not restricted to StreetNets. As of 2008, Cuba's underground market has been distributing digital materials, known as "[El Paquete Semanal](#)" ("The Weekly Package"), or "El Paquete" for short.

El Paquete consists of a [variety of digital materials](#), ranging from music, TV series, movies, and video clips, to news websites, software manuals, classifieds, and advertisements. Every week, the El Paquete package contains different materials. Cubans can purchase these packages by having the materials copied onto CDs or USB drives.

Interestingly enough, these materials [do not include pornography or any other prohibited materials](#), nor do they include content that expresses criticism towards Cuba's government. This has led some to [speculate](#) that the Cuban government might be involved in its production.

In a way, El Paquete emerged as a sort of substitute for broadband internet, serving as Cuba's "[offline internet](#)". It enables Cubans to gain access to online content, without being online.

While in Cuba, we asked where we could go to buy the weekly El Paquete. Locals directed us to a rundown building. Upon entering a family's apartment, we were guided to a room with a computer, where we could choose which digital materials we wanted to have copied onto our USB drives.

Summary

Cuba's internet landscape is quite unique for a number of reasons. For starters, it only has [one telecom company](#), which is state-owned and was only introduced to the public a few years ago. Unlike elsewhere in the world, Cubans can only access the internet in [specific designated areas](#), most of which are located in parks. The limited availability of such wifi hotspots, and the inconvenience of visiting them, in addition to the [extremely high cost of the internet](#) (especially in comparison to local salaries), constitute some of the main barriers to accessing the internet. This environment though has fostered *alternative* approaches of accessing the internet, such as the [distribution of digital materials](#) and the creation of [private mesh networks](#).

The fact that [Cuba's intranet is far more affordable](#) than the global internet indicates that most Cubans likely limit their browsing experience to government-approved sites and services. But the political climate in the country likely demands increased levels of self-censorship, which arguably is the most effective form of censorship.

In an attempt to understand how internet censorship is performed in Cuba, we performed network measurement tests across eight vantage points in three cities across Cuba. The following sections explain our methodology and key findings.

Measuring internet censorship in Cuba

We performed a variety of network measurement tests in Cuba in an attempt to understand whether and to what extent information controls are implemented.

The sections below document the methodology and findings of this study.

Methodology

The methodology of this study included the following:

- Collection and analysis of [ooniprobe](#) network measurements;
- Custom network measurement tests.

The wifi hotspots from which we performed network measurement tests were located in parks, hotels, a store and airport across Havana, Santa Clara, and Santiago de Cuba. Most of our tests were performed in ParkNets.

The analysis period started on 29th May 2017 and concluded on 10th June 2017.

Collection and analysis of ooniprobe network measurements

Since 2011, OONI has developed multiple [free and open source software tests](#), called ooniprobe, designed to measure the following:

- [Blocking of websites](#);
- Blocking of instant messaging apps ([WhatsApp](#), [Facebook Messenger](#), [Telegram](#));
- Blocking of the [Tor network](#) and [Tor bridges](#);
- Presence of [middleboxes](#);
- [Speed and performance](#) of networks.

As part of this study, the following [ooniprobe tests](#) were run from eight local vantage points in Cuba:

- [Web Connectivity](#)
- [HTTP Invalid Request Line](#)
- [HTTP Header Field Manipulation](#)
- [Vanilla Tor](#)
- [WhatsApp test](#)
- [Facebook Messenger test](#)
- [Telegram test](#)
- [Network Diagnostic Test \(NDT\)](#)
- [HTTP Host](#)
- [Meek Fronted Requests](#)

The Web Connectivity test was run with the aim of examining whether a set of URLs (included in both the [global test list](#), and the [Cuban test list](#)) were blocked during the testing period and if so, how. The Vanilla Tor test was run to examine the reachability of the [Tor network](#), while the Facebook Messenger, Telegram, and WhatsApp tests were run to examine the reachability of these instant messaging apps in Cuba during the testing period.

The HTTP Invalid Request Line and HTTP Header Field Manipulation tests were run with the aim of examining whether “middleboxes” (systems placed in the network between the user and a control server) that could potentially be responsible for censorship and/or surveillance were present in the tested networks.

The NDT test was run with the aim of measuring the speed and performance of networks in Cuba.

The sections below document how each of these tests are designed.

Web Connectivity

This test examines whether websites are reachable and if they are not, it attempts to determine whether access to them is blocked through DNS tampering, TCP/IP blocking or by a transparent HTTP proxy.

OONI’s Web Connectivity test is designed to examine URLs contained in specific [lists](#) (“test lists”) for censorship. By default, Web Connectivity examines the “[global test list](#)”, which includes a wide range of internationally relevant websites, most of which are in English. These websites fall under [30 categories](#), ranging from news media, file sharing and culture, to provocative or objectionable categories, like pornography, political criticism, and hate speech.

These categories help ensure that a wide range of different types of websites are tested. The main reason why objectionable categories (such as “pornography” and “hate speech”) are included for testing is because they are more likely to be blocked due to their nature, enabling the development of heuristics for detecting censorship elsewhere within a country.

In addition to testing the URLs included in the global test list, Web Connectivity is also designed to examine a test list which is specifically created for the country that the user is running ooniprobe from, if such a list exists. Unlike the global test list, [country-specific test lists](#) include websites that are relevant and commonly accessed within specific countries, and such websites are often in local languages. Similarly to the global test

list, country-specific test lists include websites that fall under the same set of [30 categories](#), as explained previously. All test lists are hosted by the [Citizen Lab](#) on [GitHub](#), supporting OONI and other network measurement projects in the creation and maintenance of lists of URLs to test for censorship.

As part of this study, OONI's Web Connectivity test examined the accessibility of URLs included in both the "[global test list](#)" (containing 1,109 URLs) and in the "[Cuban test list](#)" (containing 349 URLs). In total, Web Connectivity tests **measured 1,458 URLs** for censorship across eight local vantage points in Cuba between 29th May 2017 to 10th June 2017.

OONI's Web Connectivity test is designed to perform the following:

- Resolver identification
- DNS lookup
- TCP connect
- HTTP GET request

By default, this test performs the above (excluding the first step, which is performed only over the network of the user) both over a control server and over the network of the user. If the results from both networks match, then there is no clear sign of network interference; but if the results are different, the websites that the user is testing are likely censored.

Further information is provided below, explaining how each step performed under the web connectivity test works.

1. Resolver identification

The domain name system (DNS) is what is responsible for transforming a host name (e.g. torproject.org) into an IP address (e.g. 38.229.72.16). Internet Service Providers (ISPs), amongst others, run DNS resolvers which map IP addresses to hostnames. In some circumstances though, ISPs map the requested host names to the wrong IP addresses, which is a form of tampering.

As a first step, the Web Connectivity test attempts to identify which DNS resolver is being used by the user. It does so by performing a DNS query to special domains (such as whoami.akamai.com) which will disclose the IP address of the resolver.

2. DNS lookup

Once the Web Connectivity test has identified the DNS resolver of the user, it then attempts to identify which addresses are mapped to the tested host names by the resolver. It does so by performing a DNS lookup, which asks the resolver to disclose which IP addresses are mapped to the tested host names, as well as which other host names are linked to the tested host names under DNS queries.

3. TCP connect

The Web Connectivity test will then try to connect to the tested websites by attempting to establish a TCP session on port 80 (or port 443 for URLs that begin with HTTPS) for the list of IP addresses that were identified in the previous step (DNS lookup).

4. HTTP GET request

As the Web Connectivity test connects to tested websites (through the previous step), it sends requests through the HTTP protocol to the servers which are hosting those websites. A server normally responds to an HTTP GET request with the content of the webpage that is requested.

Comparison of results: Identifying censorship

Once the above steps of the web connectivity test are performed *both* over a control server and over the network of the user, the collected results are then compared with the aim of identifying whether and how tested websites are tampered with. If the compared results do *not* match, then there is a sign of network interference.

Below are the conditions under which the following types of blocking are identified:

- **DNS blocking:** If the DNS responses (such as the IP addresses mapped to host names) do *not* match.
- **TCP/IP blocking:** If a TCP session to connect to websites was *not* established over the network of the user.
- **HTTP blocking:** If the HTTP request over the user's network failed, or the HTTP status codes don't match, or all of the following apply:
 - The body length of compared websites (over the control server and the network of the user) differs by some percentage;
 - The HTTP headers names do not match;
 - The HTML title tags do not match.

It's important to note, however, that DNS resolvers, such as Google or a local ISP, often provide users with IP addresses that are closest to them geographically. Often this is *not* done with the intent of network tampering, but merely for the purpose of providing users with localized content or faster access to websites. As a result, some false positives might arise in OONI measurements. Other false positives might occur when tested websites serve different content depending on the country that the user is connecting from, or in the cases when websites return failures even though they are not tampered with (e.g. because they are overloaded).

HTTP Invalid Request Line

This test tries to detect the presence of network components ("middlebox") which could be responsible for censorship and/or traffic manipulation.

Instead of sending a normal HTTP request, this test sends an invalid HTTP request line - containing an invalid HTTP version number, an invalid field count and a huge request method - to an echo service listening on the standard HTTP port. An echo service is a very useful debugging and measurement tool, which simply sends back to the originating source any data it receives. If a middle box is not present in the network between the user and an echo service, then the echo service will send the invalid HTTP request line back to the user, exactly as it received it. In such cases, there is no visible traffic manipulation in the tested network.

If, however, a middle box is present in the tested network, the invalid HTTP request line will be intercepted by the middle box and this may trigger an error and that will subsequently be sent back to OONI's server. Such errors indicate that software for traffic manipulation is likely placed in the tested network, though it's not always clear what that software is. In some cases though, censorship and/or surveillance vendors can be identified through the error messages in the received HTTP response. Based on this technique, OONI has previously [detected](#) the use of BlueCoat, Squid and Privoxy proxy technologies in networks across multiple countries around the world.

It's important though to note that a false negative could potentially occur in the hypothetical instance that ISPs are using highly sophisticated censorship and/or surveillance software that is specifically designed to not trigger errors when receiving invalid HTTP request lines like the ones of this test. Furthermore, the presence of a middle box is not necessarily indicative of traffic manipulation, as they are often used in networks for caching purposes.

HTTP Header Field Manipulation

This test also tries to detect the presence of network components (“middlebox”) which could be responsible for censorship and/or traffic manipulation.

HTTP is a protocol which transfers or exchanges data across the internet. It does so by handling a client’s request to connect to a server, and a server’s response to a client’s request. Every time a user connects to a server, the user (client) sends a request through the HTTP protocol to that server. Such requests include “HTTP headers”, which transmit various types of information, including the user’s device operating system and the type of browser that is being used. If Firefox is used on Windows, for example, the “user agent header” in the HTTP request will tell the server that a Firefox browser is being used on a Windows operating system.

This test emulates an HTTP request towards a server, but sends HTTP headers that have variations in capitalization. In other words, this test sends HTTP requests which include valid, but non-canonical HTTP headers. Such requests are sent to a backend control server which sends back any data it receives. If OONI receives the HTTP headers exactly as they were sent, then there is no visible presence of a “middle box” in the network that could be responsible for censorship, surveillance and/or traffic manipulation. If, however, such software is present in the tested network, it will likely process and forward the request, most likely normalizing the headers capitalization and/or add extra headers.

Depending on whether the HTTP headers that are sent and received from a backend control server are the same or not, OONI is able to evaluate whether software – which could be responsible for traffic manipulation – is present in the tested network.

False negatives, however, could potentially occur in the hypothetical instance that ISPs are using highly sophisticated software that is specifically designed to not interfere with HTTP headers when it receives them. Furthermore, the presence of a middle box is not necessarily indicative of traffic manipulation, as they are often used in networks for caching purposes.

Vanilla Tor

This test examines the reachability of the [Tor network](#), which is designed for online anonymity and censorship circumvention.

The Vanilla Tor test attempts to start a connection to the Tor network. If the test successfully bootstraps a connection within a predefined amount of seconds (300 by default), then Tor is considered to be reachable from the vantage point of the user. But

if the test does not manage to establish a connection, then the Tor network is likely blocked within the tested network.

WhatsApp test

This test is designed to examine the reachability of both WhatsApp's app and the WhatsApp web version within a tested network.

OONI's WhatsApp test attempts to perform an HTTP GET request, TCP connection and DNS lookup to WhatsApp's endpoints, registration service and web version over the vantage point of the user. Based on this methodology, WhatsApp's *app* is likely blocked if any of the following apply:

- TCP connections to WhatsApp's endpoints fail;
- TCP connections to WhatsApp's registration service fail;
- DNS lookups resolve to IP addresses that are *not* allocated to WhatsApp;
- HTTP requests to WhatsApp's registration service do *not* send back a response to OONI's servers.

WhatsApp's *web interface* is likely blocked if any of the following apply:

- TCP connections to web.whatsapp.com fail;
- DNS lookup illustrates that a different IP addresses has been allocated to web.whatsapp.com;
- HTTP requests to web.whatsapp.com do *not* send back a consistent response to OONI's servers.

Facebook Messenger test

This test is designed to examine the reachability of Facebook Messenger within a tested network.

OONI's Facebook Messenger test attempts to perform a TCP connection and DNS lookup to Facebook's endpoints over the vantage point of the user. Based on this methodology, Facebook Messenger is likely blocked if one or both of the following apply:

- TCP connections to Facebook's endpoints fail;
- DNS lookups to domains associated to Facebook do not resolve to IP addresses allocated to Facebook.

Telegram test

This test is designed to examine the reachability of Telegram's app and web version within a tested network.

More specifically, this test attempts to perform an HTTP POST request, and establish a TCP connection to Telegram's access points (DCs), as well as an HTTP GET request to Telegram's web version (web.telegram.org) over the vantage point of the user. The test is triggered as blocking when connections to *all* access points defined in the [test](#) fail.

Based on this methodology Telegram's *app* is likely blocked if any of the following apply:

- TCP connections to all the tested Telegram access points fail;
- HTTP POST requests to Telegram's access points do *not* send back a response to OONI's servers.

Telegram's *web version* is likely blocked if the following applies:

- HTTP(S) GET requests to web.telegram.org do *not* send back a consistent response to OONI's servers.

Network Diagnostic Test (NDT)

NDT (Network Diagnostic Test) is designed to measure the *speed* and *performance* of tested networks.

This network performance test was originally developed by The Internet2 Project and is currently maintained by [Measurement Lab \(M-Lab\)](#). NDT is designed to measure the speed and performance of networks by connecting to M-Lab servers close to the user, and by subsequently uploading and downloading random data. In doing so, NDT collects TCP/IP low level information that is useful to examining and characterizing the quality of the network path between the user and the mLab server.

OONI utilizes an [implementation of NDT](#) for [measurement-kit](#), which is a network measurement library for running both desktop and mobile network measurement tests. This NDT implementation is included as a test that can be run via OONI's mobile apps. Running NDT can be useful as the type of information that it collects can potentially be used to examine cases of throttling.

HTTP Host

This test attempts to:

- examine whether the domain names of websites are blocked;
- detect the presence of “middleboxes” (software which could be used for censorship and/or traffic manipulation) in tested networks;
- assess which censorship circumvention techniques are capable of bypassing the censorship implemented by the “middle box”.

Every time you connect to a server, you (the client) send a request through the HTTP protocol to that server. Such requests include “HTTP headers”, some of which (the “Host header”) include information about the specific domain that you want to connect to. When you connect to torproject.org, for example, the host header of your HTTP request includes information which communicates that you want to connect to that domain.

This test implements a series of techniques which help it evade getting detected from censors and then uses a list of domain names (such as bbc.co.uk) to connect to an OONI backend control server, which sends the host headers of those domain names back to us. If a “middle box” is detected between the network path of the probe and the OONI backend control server, its fingerprint might be included in the JSON data that we receive from the backend control server. Such data also informs us if the tested domain names are blocked or not, as well as how the censor tried to fingerprint the censorship of those domains. This can sometimes lead to the identification of the type of infrastructure being used to implement censorship.

Note: The presence of a middle box is not necessarily indicative of censorship and/or traffic manipulation, as they are often used in networks for caching purposes.

Meek Fronted Requests

This test examines whether the domains used by Meek (a type of [Tor bridge](#)) work in tested networks.

Meek is a [pluggable transport](#) which uses non-blocked domains, such as google.com, awsstatic.com (Amazon cloud infrastructure) and ajax.aspnetcdn.com (Microsoft azure cloud infrastructure), to proxy its users over [Tor](#) to blocked websites, while hiding both the fact that they are connecting to such websites and how they are connecting to them. As such, Meek is useful for not only connecting to websites that are blocked, but for also hiding which websites you are connecting to.

Below is a simplified explanation of how this works:

[user] → [<https://www.google.com>] → [Meek hosted on the cloud] → [Tor] → [blocked-website]

The user will receive a response (access to a blocked website, for example) from cloud-fronted domains, such as google.com, through the following way:

[blocked-website] → [Tor] → Meek hosted on the cloud] → [<https://www.google.com>] → [user]

In short, this test does an encrypted connection to cloud-fronted domains over HTTPS and examines whether it can connect to them or not. As such, this test enables users to check whether Meek enables the circumvention of censorship in an automated way.

Data analysis

Through its [data pipeline](#), OONI processes all network measurements that it collects, including the following types of data:

Country code

OONI by default collects the code which corresponds to the country from which the user is running ooniprobe tests from, by automatically searching for it based on the user's IP address through the [MaxMind GeoIP database](#). The collection of country codes is an important part of OONI's research, as it enables OONI to map out global network measurements and to identify where network interferences take place.

Autonomous System Number (ASN)

OONI by default collects the Autonomous System Number (ASN) which corresponds to the network that a user is running ooniprobe tests from. The collection of the ASN is useful to OONI's research because it reveals the specific network provider (such as Vodafone) of a user. Such information can increase transparency in regards to which network providers are implementing censorship or other forms of network interference.

Date and time of measurements

OONI by default collects the time and date of when tests were run. This information helps OONI evaluate when network interferences occur and to compare them across time.

IP addresses and other information

OONI does *not* deliberately collect or store users' IP addresses. In fact, OONI takes measures to remove users' IP addresses from the collected measurements, to protect its users from [potential risks](#).

However, OONI might *unintentionally* collect users' IP addresses and other potentially personally-identifiable information, if such information is included in the HTTP headers or other metadata of measurements. This, for example, can occur if the tested websites include tracking technologies or custom content based on a user's network location.

Network measurements

The types of network measurements that OONI collects depend on the types of tests that are run. Specifications about each OONI test can be viewed through its [git repository](#), and details about what collected network measurements entail can be viewed through [OONI Explorer](#) or [OONI's measurement API](#).

OONI processes the above types of data with the aim of deriving meaning from the collected measurements and, specifically, in an attempt to answer the following types of questions:

- Which types of OONI tests were run?
- In which countries were those tests run?
- In which networks were those tests run?
- When were tests run?
- What types of network interference occurred?
- In which countries did network interference occur?
- In which networks did network interference occur?
- When did network interference occur?
- How did network interference occur?

To answer such questions, OONI's pipeline is designed to process data which is automatically sent to OONI's measurement collector by default. The initial processing of network measurements enables the following:

- Attributing measurements to a specific country.
- Attributing measurements to a specific network within a country.
- Distinguishing measurements based on the specific tests that were run for their collection.

- Distinguishing between “normal” and “anomalous” measurements (the latter indicating that a form of network tampering is likely present).
- Identifying the type of network interference based on a set of heuristics for DNS tampering, TCP/IP blocking, and HTTP blocking.
- Identifying block pages based on a set of heuristics for HTTP blocking.
- Identifying the presence of “middleboxes” within tested networks.

However, false positives emerge within the processed data due to a number of reasons. As explained in the previous section, DNS resolvers (operated by Google or a local ISP) often provide users with IP addresses that are closest to them geographically. While this may appear to be a case of DNS tampering, it is actually done with the intention of providing users with faster access to websites. Similarly, false positives may emerge when tested websites serve different content depending on the country that the user is connecting from, or in the cases when websites return failures even though they are not tampered with.

Furthermore, measurements indicating HTTP or TCP/IP blocking might actually be due to temporary HTTP or TCP/IP failures, and may not conclusively be a sign of network interference. It is therefore important to test the same sets of websites across time and to cross-correlate data, prior to reaching a conclusion on whether websites are in fact being blocked.

Since instances of internet censorship differ from country to country and sometimes even from network to network, it is quite challenging to accurately identify them. OONI uses a series of heuristics to try to examine whether a measurement differs from the expected control, but these heuristics can often result in false positives (as explained in the previous section). As a result, ***OONI only confirms instances of blocking when block pages are detected.***

OONI’s methodology for detecting the presence of “middleboxes” - systems that could be responsible for censorship, surveillance and traffic manipulation - can also present false negatives, if ISPs are using highly sophisticated software that is specifically designed to *not* interfere with HTTP headers when it receives them, or to *not* trigger error messages when receiving invalid HTTP request lines. It remains unclear though if such software is being used. Moreover, it’s important to note that the presence of a middle box is not necessarily indicative of internet censorship, as such systems are often used in networks for caching purposes.

OONI continues to develop its data analysis heuristics to identify internet censorship events faster and more accurately.

Custom tests

As part of our testing in Cuba, we also wrote and ran various custom network measurement tests, in addition to running [ooniprobe](#). These included traceroutes, DNS queries, and network scans, as well as custom tests measuring the latency to blocked sites and other follow-up tests in response to ooniprobe findings.

The main test that yielded interested findings (included under the “Findings” section of this report) was a custom test that we wrote to measure the latency to blocked sites. This test, in particular, is designed to measure the latency when connecting to blocked sites. If the latency is low, we can infer that the equipment used to implement the censorship is geographically close to the user running this test. If, however, the latency when connecting to blocked sites is high, then the censorship equipment is more likely located in a further geographical location.

Findings

Upon analysis of the collected [network measurements](#), we can confirm the **blocking of 41 websites** in Cuba. Deep Packet Inspection (DPI) technology, which appears to be located in Havana based on latency measurements, was found to reset connections to those sites and serve (blank) block pages. Only the HTTP version of those sites was blocked, potentially enabling users to circumvent the censorship by merely accessing them over HTTPS.

Most of the blocked sites express criticism towards Cuba’s government, either directly or indirectly. While various web proxies were found to be blocked, it’s worth noting that the [Tor network](#) was found to be [accessible](#) across Cuba. Similarly, popular communications tools, like [Facebook Messenger](#) and [WhatsApp](#), were found to be accessible. Skype was the only popular communications tool that we found to be blocked.

Chinese vendor Huawei was found to be supporting Cuba’s internet infrastructure, but it remains unclear if it is implementing internet censorship in the country. What is clear though is that Google appears to be blocking access to Google App Engine from Cuba.

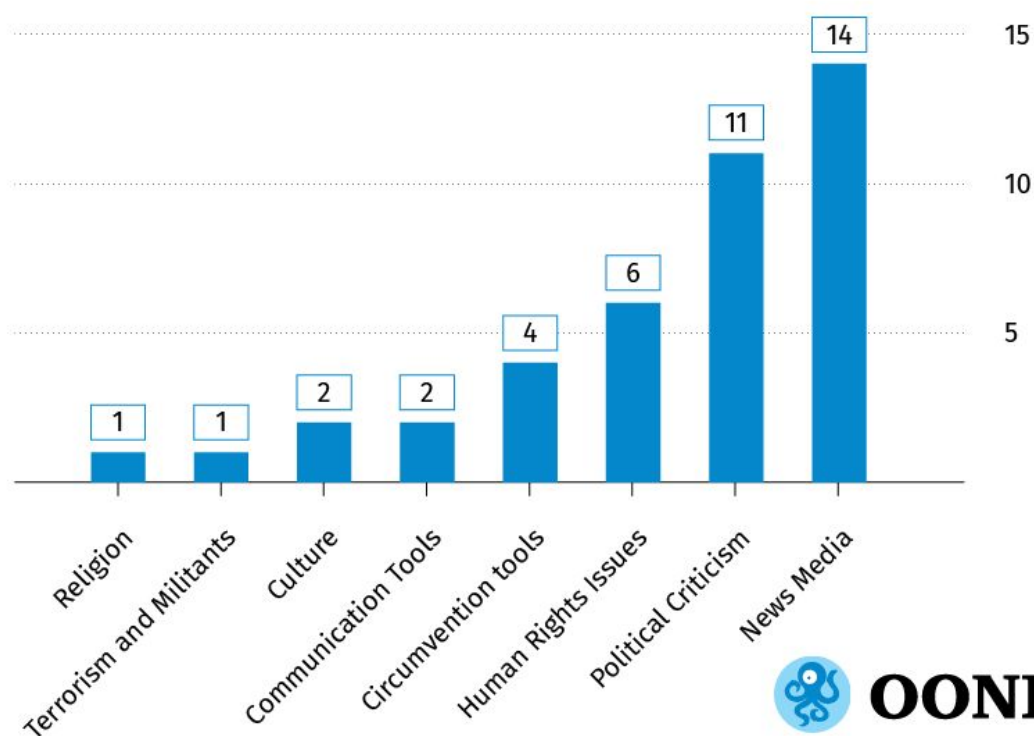
The sections below provide more information pertaining to the censorship events that we found in Cuba as part of this study.

Blocked websites

News outlets and sites expressing political criticism towards Cuba's government were predominantly found to be blocked as part of this study. Upon analysis of [network measurement data](#) collected through [OONI's Web Connectivity test](#) (performed across eight vantage points in Havana, Santa Clara, and Santiago de Cuba), we were able to identify and confirm the **blocking of 41 websites**. We also found that these sites are blocked by Deep Packet Inspection (DPI) technology which reset connections and served (blank) block pages. It's worth emphasizing that only the HTTP version of these sites was found to be blocked. While, in theory, users could potentially circumvent the censorship over HTTPS, many of the sites found to be blocked do not support HTTPS.

Below we illustrate the amount of types of sites found to be blocked in Cuba as part of this study.

Types of sites blocked in Cuba



Through the above chart, it is evident that news outlets and sites expressing political criticism were found to be blocked the most.

Below we include a table which lists all 41 sites that we confirmed to be blocked in Cuba during the testing period. In the third column of the table, we list the amount of times that we detected block pages for each site. It's worth noting that all of the following sites presented block pages every single time we tested them across eight vantage points in Havana, Santa Clara, and Santiago de Cuba.

Blocked websites	Types of sites	Times found blocked
http://anon.inf.tu-dresden.de	Anonymity and circumvention tools	11
http://anonymouse.org	Anonymity and circumvention tools	10
http://www.inetprivacy.com	Anonymity and circumvention tools	8
http://www.megaproxy.com	Anonymity and circumvention tools	1
http://www.callserve.com	Communication Tools	7
http://www.pc2call.com	Communication Tools	9
http://www.vitral.org	Culture	14
http://www.cubanuestra.nu	Culture	21
http://www.cubasindical.org	Human Rights Issues	19
http://www.damasdeblanco.com	Human Rights Issues	16
http://www.hermanos.org	Human Rights Issues	21
http://www.hispanocubana.org	Human Rights Issues	20
http://www.sigloxxi.org	Human Rights Issues	17
http://freedomhouse.org/country/cuba	Human Rights Issues	12
http://www.lanuevacuba.com	News Media	18
http://martinoticias.com	News Media	18
http://miscelaneasdecuba.net	News Media	20
http://www.cartadecuba.org	News Media	19
http://www.cubaencuentro.com	News Media	42
http://www.cubafreepress.org	News Media	21
http://www.cubalibredigital.com	News Media	19

http://www.cubamatinal.com	News Media	18
http://www.cubaliberal.org	News Media	21
http://www.netforcuba.org	News Media	20
http://www.nuevoaccion.com	News Media	18
http://www.payolibre.com	News Media	18
http://www.voanews.com	News Media	19
http://www.14ymedio.com/	News Media	17
http://conexioncubana.net	Political Criticism	20
http://cubanology.com	Political Criticism	19
http://pscuba.org	Political Criticism	19
http://www.agendacuba.org	Political Criticism	21
http://www.asambleasociedadcivilcuba.info	Political Criticism	17
http://www.cubademocraciayvida.org	Political Criticism	18
http://www.cubaeuropa.com	Political Criticism	20
http://www.corriente.org	Political Criticism	20
http://www.directorio.org	Political Criticism	18
http://www.therealcuba.com/	Political Criticism	16
http://www.solidaridadconcuba.com	Political Criticism	17
http://www.idealpress.com	Religion	18
http://www.alpha66.org	Terrorism and Militants	19

The following sections provide further information pertaining to the blocking of sites, as found through this study.

News Media

Fourteen news websites were confirmed to be blocked in Cuba during the testing period, as illustrated through the table below.

Blocked media websites	Amount of block pages detected
http://martinoticias.com	18
http://miscelaneasdecuba.net	20
http://www.cartadecuba.org	19
http://www.cubaencuentro.com	42
http://www.cubafreepress.org	21
http://www.cubalibredigital.com	19

http://www.cubamatinal.com	18
http://www.cubaliberal.org	21
http://www.netforcuba.org	20
http://www.nuevoaccion.com	18
http://www.payolibre.com	18
http://www.voanews.com	19
http://www.14ymedio.com/	17
http://www.lanuevacuba.com	18

Most of the above news websites express political criticism towards Cuba’s government, possibly explaining the motivation behind their censorship.

[Radio and TV Marti](#), for example, is an independent news outlet which aims to “provide the Cuban people with news and information without the censorship of the Cuban government”. As part of its reporting on Cuba, Radio and TV Marti frequently [covers human rights issues](#), including the arrest of activists. Similarly, [Cuba Encuentro](#) is a news outlet that, amongst other topics, [reports on human rights issues](#) in Cuba, with a focus on LGBT rights and women’s rights. In addition to news articles, Cuba Encuentro [publishes](#) documents, legislation, opinion articles, and videos on issues that are more relevant to women and Cuba’s LGBT community. Along with [Radio and TV Marti](#), [Cuba Encuentro was found to be blocked](#) in Cuba as well.

Cuba’s first independent online news outlet (created in 1997), [La Nueva Cuba](#), was also found to be [blocked](#). This site is no longer operational, and (when accessed outside of Cuba) its domain redirects to “Havana City Hotels”. The image below, taken from the [Internet Archive](#), shows what La Nueva Cuba used to look like, when it operated as a news site.



Source: Internet Archive, La Nueva Cuba,

<https://web.archive.org/web/20050831051647/http://www.lanuevacuba.com:80/master.htm>

La Nueva Cuba used to feature articles covering human rights issues, such as violence against political dissidents, possibly explaining why it was ultimately shut down.



Source: Internet Archive, La Nueva Cuba,

<https://web.archive.org/web/20050831211614/http://www.lanuevacuba.com:80/oposicion-debate.htm>

[Yoani Sanchez](#), a Cuban blogger who received international fame for her [critical portrayal of life in Cuba](#) under its current government, co-founded the next independent Cuban news outlet: [14ymedio](#). In light of limited internet availability, [Cuban 14ymedio journalists collaborate with a small team outside of Cuba](#), who upload their articles and help coordinate social media efforts. This news site though was also found to be [blocked](#) in Cuba.

[Cuba Libre Digital](#), run by the Cuban diaspora in Brazil, is another independent news outlet [blocked](#) in the country. [PayoLibre](#), which has [published articles in defense of political dissidents](#), was found to be [censored](#). Netforcuba.org, also [blocked](#), currently points to a YouTube page which includes a video report titled “Cuba, false paradise”.

Limited press freedom in Cuba led to the creation of the [Cuba Free Press Project](#). This initiative [aims to support journalists and independent writers](#), providing them a platform for free expression. This was also amongst the sites found to be [blocked](#). Quite similarly, news site [Nuevo Accion](#) supports independent journalism and welcomes opinion pieces from the public. The only international news site that we found to be [blocked](#) in Cuba was [Voice of America \(VOA\)](#), which is U.S. government-funded.

[ETECSA](#) appears to continue to censor sites even once they’re no longer operational. [Cubamatinal.com](#), [cubaliberal.org](#), and [miscelaneasdecuba.net](#) were all found to be [blocked](#), even though these sites are down. We also found [cartadecuba.org](#) to be [blocked](#), despite the site no longer being operational.

We only found the HTTP version of these fourteen media sites to be blocked. Out of all of them, only [Cuba Encuentro](#) and [Voice of America \(VOA\)](#) currently support HTTPS, enabling their readers to circumvent the censorship.

Political Criticism

Eleven other sites expressing political criticism towards Cuba’s government were [found to be blocked](#), as illustrated through the table below.

Blocked sites expressing political criticism	Amount of block pages detected
http://conexioncubana.net	20
http://cubanology.com	19
http://pscuba.org	19

http://www.agendacuba.org	21
http://www.asambleasociadadcivilcuba.info	17
http://www.cubademocraciayvida.org	18
http://www.cubaeuropa.com	20
http://www.corriente.org	20
http://www.directorio.org	18
http://www.therealcuba.com/	16
http://www.solidaridadconcuba.com	17

[The Real Cuba](#), a blog that expresses intense political criticism, portrays Cuba within the context of oppression. It criticizes Cuba's [healthcare](#) and [education](#) system, and describes [racism against Afro-Cubans](#). It argues that, under the Castro regime, Cuba has [more poverty than ever before](#), heavily criticising Castro's [excessive wealth](#). Overall, this blog expresses [heavy criticism towards the Castro government](#), and we found it to be [blocked](#) across Cuba.

[Conexion Cubana](#) is a Cuban online forum, providing a platform for [political discussions](#) (amongst other discussions), which we also found to be [blocked](#).

[Cuba Democracia y Vida](#) was created by Guillermo Milan Reyes, a Cuban political dissident living in exile in Sweden. This site [aims](#) to provide "a voice for all those who fight in a peaceful way, for democracy in Cuba, free from the dictatorship of Fidel Castro and for a dignified life without poverty for all Cuban citizens". To this end, it encourages Cubans to submit articles that cover news about important events, testimonies of life under the Castro regime, and reports on human rights violations. We found this site to be [blocked](#) in Cuba.

The [Cuban Democratic Directory](#) is an organization, based in the U.S., that [aims](#) to promote democracy in Cuba. To this end, it provides humanitarian and material aid to civil society organizations that resist Castro's regime. It also facilitates the exchange of information and international solidarity with the civic resistance in Cuba. According to the Cuban Democratic Directory, they are [committed](#) to promoting freedom and the respect for human rights in Cuba. Their [site](#) was amongst those that we found to be [blocked](#) in the country. Quite similarly, [Solidaridad Espanyola con Cuba](#), also [blocked](#), is run by Spaniards who [aim](#) to support a peaceful transition to democracy in Cuba.

Cubanology.com, pscuba.org, agendacuba.org, asambleasociadacivilcuba.info, cubaeuropa.com, and corriente.org are no longer operational. Yet, they were amongst the sites that we found to be [blocked](#) in Cuba during the testing period of this study.

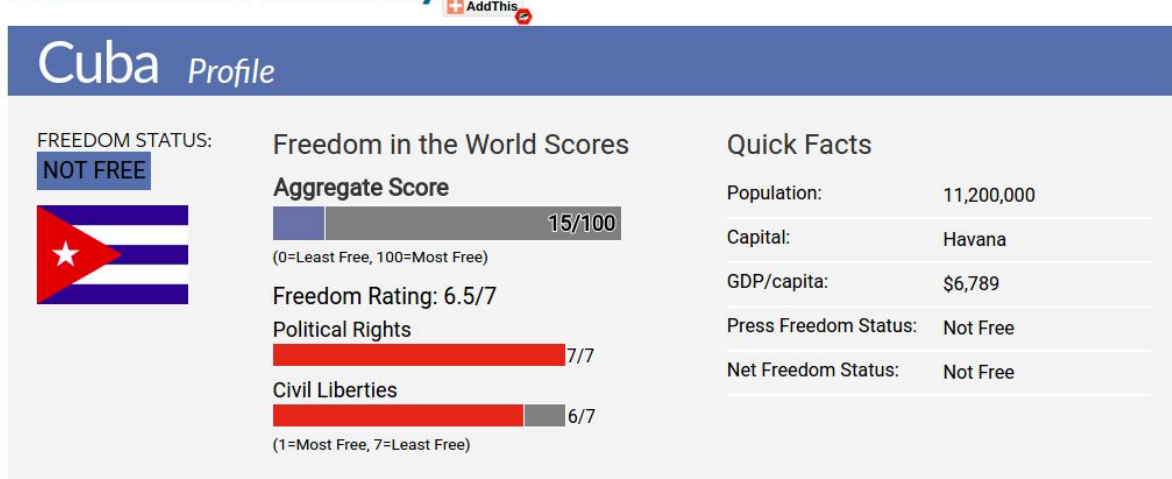
Human Rights Issues

Six sites covering human rights issues in Cuba were found to be [blocked](#) during the testing period.

Blocked human rights sites	Amount of block pages detected
http://www.cubasindical.org	19
http://www.damasdeblanco.com	16
http://www.hermanos.org	21
http://www.hispanocubana.org	20
http://www.sigloxxi.org	17
http://freedomhouse.org/country/cuba	12

[Freedom House](#) publishes annual reports on civil liberties, press freedom and internet freedom for most countries around the world, including Cuba. Its [2017 report on Cuba](#) portrayed the country as “Not Free”. The research group attributed this status to Cuba by measuring the protection of political rights and civil liberties on a scale of 1-7, where 1 is “Most Free” and 7 is “Least Free”. Overall, the country received a score of 15/100, where 0 is “Least Free” and 100 is “Most Free”, placing it amongst the “Least Free” countries in the world.

Freedom in the World 2017



Source: Freedom House, Cuba 2017 report, <https://freedomhouse.org/report/freedom-world/2017/cuba>

Freedom House also regularly publishes press releases which cover human rights issues in Cuba, such as the [crackdown on human rights defenders](#). As part of our study, we found Freedom House’s domain - including its reports on Cuba - to be [blocked](#) in the country.

But local human rights sites were found to be blocked as well. [Las Damas de Blanco](#) (“Ladies in White”) is an opposition movement founded in Cuba by the wives and other female relatives of jailed dissidents. This movement emerged following the [Black Spring](#) in 2003, when the government imprisoned 75 dissidents (including journalists, librarians, and human rights activists) on the basis that they were acting as agents of the United States. Ever since, the wives and female relatives of imprisoned dissidents have been [protesting peacefully](#) on the streets, dressed in white clothing and carrying flowers. They are united by a [common goal](#): to march peacefully demanding the freedom of their husbands, parents, children, brothers, and nephews.



Source: Las Damas de Blanco, <http://www.damasdeblanco.com/actividades/actividades.asp>

Despite protesting peacefully, they have been subjected to harassment. Recently, for example, it was [reported](#) that they were attacked by a government sanctioned mob in Havana. Their [site](#), which includes news articles and information about political prisoners, was found to be [blocked](#) in Cuba during the testing period of this study.

[Hermanos Al Rescate](#) (“Brothers to the Rescue”) is a Miami-based activist non-profit organization run by Cubans in exile who [aim](#) to “promote and support the efforts of the Cuban people to free themselves from dictatorship through the use of active

non-violence”. Formed in May 1991 following the death of a 15-year-old Cuban who tried to flee Cuba on a raft, an [integral part of their efforts](#) is to “save the lives of refugees escaping the island” and to “assist the families of political prisoners”. Hermanos Al Rescate were amongst several other Cuban-American groups that were [spied upon and infiltrated by Cuban intelligence officers](#), known as the “Cuban Five” (or the “Miami Five”). As such, it’s probably not surprising that we found their site to be [blocked](#) in Cuba.

[Fundacion Hispano Cubana](#) (“The Hispano Cubana Foundation”) is a non-profit organization which [aims](#) to enhance the protection of human rights in Cuba, as well as provide support for Cuban refugees in Spain. It also strives to promote “values of freedom and democracy in all matters relating to relations between Spain and Cuba”. While performing tests in Cuba, we found this site to be [blocked](#).

[Cuba Sindical](#) is a non-partisan, non-profit, non-governmental organization, run by the International Group for Corporate Social Responsibility in Cuba. According to its [site](#), Cuba Sindical is “dedicated to promoting free and democratic trade unionism in Cuba” and “seeks international support and solidarity for Cuban workers”. This site was most likely [blocked](#) because the Cuban government [prohibits independent trade unions](#).

Even though sigloxxi.org is not operational, we found it to be [blocked](#) as well during the testing period.

Anonymity and Circumvention Tools

The [Tor network](#) was found to be [accessible](#) across Cuba. Similarly, we were able to access other circumvention tool sites, such as [Psiphon](#). However, we found the [Java Anon Proxy](#), also known as JAP or JonDonym, to be [blocked](#), along with web proxies.

Blocked circumvention tool sites	Amount of block pages detected
http://anon.inf.tu-dresden.de	11
http://anonymouse.org	10
http://www.inetprivacy.com	8
http://www.megaproxy.com	1

[Anonymouse](#) is a popular web proxy. It enables its users to [browse the web anonymously](#), send [anonymous emails](#), and to [anonymously post entries](#) in newsgroups. MegaProxy is another web proxy which allows its users to surf the web

through a web SSL VPN service. Both were found to be [blocked](#) in Cuba during the testing period of this study, along with [iNetPrivacy software](#).

Communication Tools

Facebook Messenger is really [popular](#) in Cuba. As part of our testing, we found it to be [accessible](#) across eight vantage in the country. We also found WhatsApp to be [accessible](#).

However, we found the following communication tool sites to be blocked, even though they are no longer operational.

Blocked communication tool sites	Amount of block pages detected
http://www.callserve.com	7
http://www.pc2call.com	9

Culture

As part of this study, we also found two cultural sites to be [blocked](#).

Blocked cultural sites	Amount of block pages detected
http://www.vitral.org	14
http://www.cubanuestra.nu	21

[Vitral](#) is a socio-cultural magazine, run by the Diocese of Pinar del Rio, which aims to provide a platform for “communication, reflection, and dialogue” on Cuban culture and society. [Cuba Nuestra](#), on the other hand, is the blog of Swedes, who describe their experiences from living in Cuba (but also share stories from life in Sweden).

Religion

[IDEAL magazine](#) is a religious site that [aims](#) to “promote democracy and freedom linked to Christian thought”. To this end, it publishes articles, reports, comments, testimonies, poetry and humor in relation to Cuba and the Christian faith. As part of this study, we found it to be [blocked](#).

Blocked religious site	Amount of block pages detected
http://www.idealpress.com	18

Militant

Alpha 66 (named after its 66 original members) is an anti-Castro paramilitary group, based in Miami. Along with [Brothers to the Rescue](#) and other anti-castro groups led by Cubans in exile, it was [infiltrated by Cuban intelligence officers](#) in the 1990s.

Blocked militant site	Amount of block pages detected
http://www.alpha66.org	19

Even though the site is no longer operational (and has been squatted), ETECSA continues to [block](#) access to its domain.

Skype blocked

We found Skype to be blocked in Cuba by means of RST injection. We were able to confirm that the RST packet was injected from Cuba because the timing was much less than that of the SYN-ACK round-trip time and had an inconsistent Time To Live (TTL).

We reached this conclusion by examining packet traces. We can estimate the round-trip time by measuring the time elapsed from the moment that we send the first TCP packet (the SYN packet) until we receive the corresponding confirmation packet from the server (the SYN|ACK packet). This estimate is a baseline for the time after which we expect to receive a confirmation packet from any packet that we send over the TCP session. In normal circumstances, the time between any packet and the corresponding confirmation packet cannot be lower than the time measured initially.

Yet, we noticed that RST packets were received much faster than expected, indicating that such packets were injected by some middle box close to us, given the low latency. We also noticed that the TTL field in the RST packet was not consistent with the TTL of previously received legitimate packets. This is also a sign that the RST packet was most likely injected.

Deep Packet Inspection (DPI) technology

Once we detected the blocking of sites and services based on ooniprobe tests, we subsequently wrote a new network measurement test (called “latency-to-blocked”) that

is designed to measure the latency to the blocking infrastructure by performing test connections to a control vantage point.

Interestingly enough, this test showed low latency when connecting to blocked sites in Havana. The same test, however, presented higher latency from Santa Clara, and even higher latency from Santiago de Cuba. This allowed us to infer that the censorship equipment used in Cuba is most likely located in Havana (and in any case, for sure in Cuba).

Based on the latency measurements (and other measurements collected through [OONI's HTTP Host test](#)), we were able to confirm that Deep Packet Inspection (DPI) technology was used to block access to sites and services in Cuba. Through packet captures done on the server-side, we found that the request of the client never arrived and was RST by the DPI middlebox, as illustrated below.

268	77.961069	152.206.141.82	199.119.112.184	TCP	78	34045-80	[SYN]	Seq=0	Win=65535	Len=0	MSS=1320	WS=32	TSval=98503
269	77.961109	199.119.112.184	152.206.141.82	TCP	74	80-34045	[SYN, ACK]	Seq=0	Ack=1	Win=28960	Len=0	MSS=1460	SACK_P
270	78.087215	152.206.141.82	199.119.112.184	TCP	66	34045-80	[ACK]	Seq=1	Ack=1	Win=132096	Len=0	TSval=985033421	TSe
271	78.088759	152.206.141.82	199.119.112.184	TCP	54	34045-80	[RST]	Seq=1	Win=0	Len=0			

Moreover, we found that the connection was also RST (after having served the injected blockpage) on the client as well.

To further understand the characteristics of the DPI technology, we wrote a test that sends a packet only containing the blocked domain. The purpose of this experiment was to understand whether the blocking equipment was processing HTTP or was just reacting to the presence of a censored domain inside a packet. After some iterations, we discovered that, to trigger the blocking, it was enough to send a packet only containing a colon (":") followed by a space, followed by the blocked domain, and followed by a newline (specifically the internet newline, composed of the CR and LF characters).

On the contrary, sending the domain followed by newline, but not prefixed by a colon and a space did not trigger the reset. This confirmed our initial hypothesis that the censorship equipment only reacts to specific strings present in the packets and does not bother with processing actual HTTP messages. As a possibly unintended consequence, this means that censorship will be triggered if the blocked domain is included in any HTTP header, since the string triggering blocking does not check whether the blocked domain is part of an HTTP message and inside of the "Host" header.

Huawei equipment in Cuba

[Huawei](#), a Chinese multinational networking and telecommunications equipment and services company, appears to have supported Cuba's internet infrastructure. And this was evident without even running any network measurement tests.

When accessing blocked websites in Cuba, for example, we noticed that the server header contained the following value: **V2R2C00-IAE/1.0**. This version string appears to be [associated to Huawei equipment called eSight](#), which is generally a “[unified software suite for planning, operating, and maintaining complex enterprise ICT infrastructure](#)”.

Interestingly enough, ETECSA's login portal - through which Cubans access the internet - appears to have been written by Chinese developers, since its source code contains comments written in Chinese. This indicates that ETECSA likely hired Chinese developers to implement the portal.

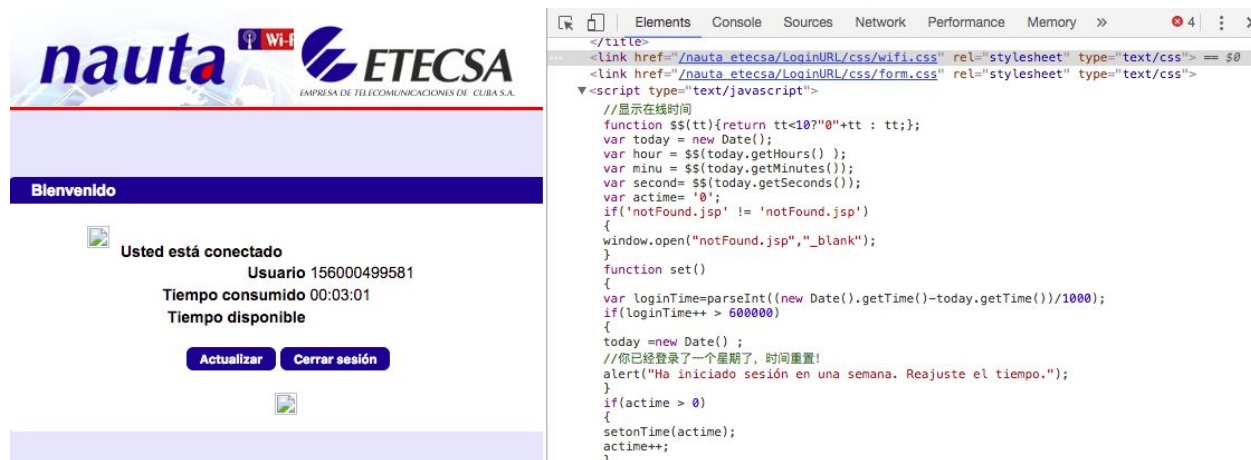


Image: ETECSA login page containing Chinese comments in source code

We also noticed that the server of the captive portal replies with the following server header: **OpenAS**. This too is [associated to Huawei equipment](#).

While it's clear that Cuba is using Huawei access points, it remains unclear to us whether and to what extent Huawei equipment is actually being used to implement internet censorship in the country.

Google App Engine blocked by Google

To measure the speed and performance of networks in Cuba, we attempted to run [OONI's Network Diagnostic Test \(NDT\)](#). This test is designed to measure the speed and performance of networks by connecting to [M-Lab](#) servers close to the user, and by subsequently uploading and downloading random data. In doing so, NDT collects TCP/IP low level information that is useful to examining and characterizing the quality of the network path between the user and the M-Lab server.

However, we were initially unable to run the NDT test in any networks in Cuba. Upon examination, we realized that this is due to the fact that M-Lab uses Google App Engine to discover the closest server to the user. And Google App Engine appeared to be blocking IP addresses originating from Cuba. In other words, we found that Google was blocking access to Google App Engine from Cuba.

We later worked around the problem by manually specifying the test servers connected to by NDT. This allowed us to avoid using M-Lab services which rely on Google App Engine (which was blocked), and to directly connect to test servers instead.

Acknowledgement of limitations

The findings of this study present various limitations.

While [OONI network measurements](#) have been collected from Cuba since January 2016, this study only analyzes recent network measurements collected between 29th May 2017 to 10th June 2017. As such, censorship events which may have occurred before and/or after this testing period are not analysed as part of this study.

Another limitation is associated to the amount and types of URLs that were tested for censorship. As mentioned in the methodology section of this report, [OONI's Web Connectivity test](#) was run to examine the accessibility of [349 URLs](#) that are more relevant to the Cuban context and [1,109 internationally relevant sites](#). While a total of 1,458 URLs were tested for censorship as part of this study, we did not test all of the URLs on the internet, indicating the possibility that other websites not included in [tests lists](#) might have been blocked.

Finally, while network measurements were collected from eight local vantage points across three cities in Cuba, tests were not run from every vantage point possible in the

country. Therefore, the findings of this study are limited to the vantage points from which network measurement tests were run.

Conclusion

[OONI data](#) collected from Cuba confirms the **blocking of 41 websites**. Most of these sites include news outlets and blogs, as well as pro-democracy and human rights sites. Many of the blocked sites, directly or indirectly, express criticism towards Castro's regime. Interestingly enough though, various other international sites which also express criticism - such as Reporters Without Borders' [portrait of Cuba's President](#), presenting him as a "Predator of Press Freedom" - were found to be [accessible](#) across Cuba.

Web proxies, like [Anonymouse](#), were amongst those found to be blocked, limiting Cubans' ability to circumvent censorship. It's worth noting though that the [Tor anonymity network](#) was found to be [accessible](#) across the country. This is likely due to the fact that [Cuba has relatively few Tor users](#).

Deep Packet Inspection (DPI) technology was found to be blocking sites by resetting connections and serving (blank) block pages. Through latency measurements, we were also able to confirm that the blocking server is most likely located in Havana (and in any case, for sure in Cuba). Only the HTTP version of sites was found to be blocked. While, in theory, Cubans could potentially circumvent the censorship by merely accessing such sites over HTTPS, many of the sites found to be blocked do not support HTTPS.

Skype was the only popular communications tool that we found to be censored. By examining packet traces, we were able to determine that the DPI middlebox blocked Skype by means of RST injection. Other popular communications tools, such as [Facebook Messenger](#) and [WhatsApp](#), were accessible.

Huawei, a Chinese multinational networking and telecommunications equipment and services company, was found to be supporting Cuba's internet infrastructure. The server header of blocked sites, for example, pointed to Huawei equipment. While it is clear that Cuba is using Huawei's access points, it remains unclear whether and to what extent the company is actually implementing internet censorship in the country. What was clear though was that Google is blocking access to Google App Engine from Cuba.

Internet censorship in Cuba does *not* appear to be particularly sophisticated. Cuba's ISP only appears to be blocking the HTTP version of sites, enabling users to potentially

circumvent censorship by accessing such sites over HTTPS. While Cuba's ISP targets *some* sites that are viewed as overly critical of its government, many other international websites which also express criticism are not censored. Given the [high cost of the internet](#), rendering it inaccessible to most Cubans, perhaps the government doesn't even *need* to invest in sophisticated internet censorship.

On average, [Cubans earn around 25 CUC per month](#), while only 1 hour of internet access [costs 1.5 CUC](#). Cuba's *intranet* is more than ten times cheaper (at [0.10 CUC](#) per hour), indicating that many Cubans possibly limit their browsing experience to government-approved sites and services. The high cost of the internet, and the [limited availability of ParkNets](#) (or other public wifi hotspots) across the country, remain the main barriers to accessing the internet in Cuba.

Cuba's environment has fostered *alternative* approaches of accessing the internet. Multiple private mesh networks, known as "[StreetNets](#)", have sprung across Havana and other Cuban cities. An "[offline internet](#)" has emerged through underground markets, providing Cubans access to online content, without being online.

Cuba's internet landscape has changed quite a lot over the last years, and it will likely continue to evolve. But so might internet censorship. It is therefore important to continue to measure networks. Software like [ooniprobe](#) allows users in Cuba and beyond to collect data that sheds light on information controls.



Image by Arturo Filastò (CC-BY-SA-3.0)