THE YEAR IN REVIEW
2016

#Filterwatch

Iranian Internet Infrastructure and Policy Report

A Small Media report bringing you the year in review on internet policy and online censorship direct from Iran.

smallmedia.org.uk

This work is licensed under a Creative Commons Attribution-NonCommercial 3.0 Unported License
ABOUT US
Small Media is an organisation working to support civil society development and human rights advocacy in the MENA region. We do this by providing research, design, training, and technology support to our partners, and by working with them to develop effective and innovative digital advocacy strategies and campaigns. We also provide digital security support to a range of partners to ensure that they can work safely and securely.

Our IIIP series provides a technically minded overview of Iranian internet policy as it develops under President Rouhani, with a focus on the emerging National Internet, surveillance technologies, and online censorship. These reports stretch back to early 2013, providing an unparalleled overview of changing internet policy in the Islamic Republic.

Research team
Kyle Bowen
Mo Hoseini
James Marchant
Tom Ormson
Amin Sabeti

Design team
Richard Kahwagi
Surasti Puri
Introduction

It has been a rollercoaster of a year in Iran’s ICT sector. The first phase of the long-awaited National Information Network (SHOMA) was launched at the end of August, Telegram remains the focus of contentious debate among officials and governmental bodies, and the Iranian government continues to work to populate online space with more ‘Islamic content’.

In an effort to encapsulate the key internet policy developments of 2016, Small Media presents this comprehensive annual report, which contains a number of in-depth features from our 2016 Iranian Internet Policy and Infrastructure (IIIP) reports and three new pieces tracking developments in key policy areas – the implementation of SHOMA, the status of Telegram, and Iran’s push to develop domestic online services. These stories track the key announcements and policy initiatives from ministers, government bodies and civil society organisations over the course of the year, and follow their progress (or lack thereof) as well as the institutional conflicts that have emerged.
Iranian Internet Policy in 2016 //
An Overview

January saw officials conceding that 67% of Iranians make use of internet circumvention tools. As well as confirming that Iranian authorities are well aware of the futility of existing censorship policy, the announcement underlined the government’s stated priority of developing high-quality, domestically produced online platforms to draw Iranian users away from global alternatives. January also saw the signing of a partnership agreement between China and Iran for further cooperation in the ICT sector.

An Internet World Stats report released in February ascertained that the number of Iranian internet users increased from 250,000 in 2000 to 46,800,000 in 2015, placing internet penetration rates at 57.2%. February also saw another agreement signed, this time between Afghanistan and Iran, for the development of fiber optic networks between the two countries.

In March, we learned that the ICT Ministry had spent 1 trillion IRR (33 million USD) on its so-called ‘Intelligent Filtering’ project—ostensibly designed to identify and selectively filter forbidden online content without blocking entire websites—although no progress had been made on the implementation of the censorship system. Iran’s Cyber Police (FATA) also warned individuals against advertising hacking tools over social media networks, after claims that Telegram was being used to solicit them.

April saw the government devote yet more energy to devising filtering policies, with ICT Minister Mahmoud Vaezi claiming that Telegram would close pornographic channels within 24 hours of a request from the Iran’s government. Meanwhile, officials restated their commitment to the regulation of online dating.

At a meeting in May the Supreme Council of Cyberspace (SCC) voted in favour of a measure requiring all messaging apps to move their servers to Iran within a year in order to continue operating. In May Iran’s parliament also passed a law banning the advertisement of illegal and ‘harmful’ goods and services on social media.

SHOMA was a hot topic in June, with a series of hardline politicians claiming that delays to the national network were allowing the internet to inflict substantial damage on society. The Rouhani administration responded by promising that the first phase of SHOMA would be concluded by September.

Iranian mobile operator Irancell was hacked in July and a database with the information of 20 million users was shared on Telegram. The ICT Ministry also ruled that Internet Service Providers (ISPs) have to separate international traffic from domestic traffic for billing purposes, with users paying less for domestic traffic.

Late August saw the launch of the first phase of SHOMA, with a promise of quality internet access and a high quality, secure digital infrastructure for domestically hosted services. There was also a call for the creation of a new legal system to regulate cyberspace.

Social media networks bore the brunt of September, with the Commission to Determine the Instances of Criminal Content (CDICC) secretary Abdolsamad Khoramabadi claiming that all social media networks active in Iran are developed and operated by the “Zionist Regime”, as a reference to Israel. On top of this, the ICT Ministry said there were no plans to move Telegram servers inside Iran, contradicting the May SCC vote. In October FATA announced that they had blocked 700 online dating websites that had not received licenses, as per the guidelines announced in April. This month also saw an announcement that a plan was in development to ban the use of smartphones in parliament unless they have been produced inside Iran.

The ICT Ministry hailed the successes of Intelligent Filtering in November, with the claim it had been used to filter 95 million items of sexual content on Instagram. An agreement was also signed with the Slovenian ICT Ministry to engage in further collaboration in the ICT and nanotechnology sectors.

Yet more attention was placed on Telegram in December. The Communications Regulatory Authority (CRA) said that as long as Telegram followed the laws and regulations of Iran, they would not need to move their servers inside Iran. The biggest news of the month was Rouhani’s unveiling of the Charter on Citizens Rights, which theoretically provided for numerous rights and freedoms for Iranian citizens.

# Filterwatch 2016 Review // Spotlight

The following chapters contain the highlights of our policy analysis features from our 2016 Iranian Internet Infrastructure and Policy (IIIP) reports from 2016. These pieces are published on a monthly basis to provide in-depth analysis on a number of key policy areas, ranging from Iran’s ‘National Internet’ to the health of its nascent tech startup sector.

For all the latest updates on Iranian internet policy and infrastructure development throughout 2017, be sure to check out our #Filterwatch series at smallmedia.org.uk/work/filterwatch.
February 2016 //
Iran’s Cyber Army: Phishing and Malware Campaigns Against Civil Society Organisations (CSOs)

In February’s report, we examined the role of Iran’s Cyber Army in undertaking digital attacks globally. In particular, we focused on the ways state-sponsored hackers target activists, journalists, and civil society organisations.

We’ll start with a quick overview of Iran’s offensive cyber activities, focusing specifically on phishing attacks aimed at information gathering. Then we’ll look at some recent attacks and techniques in a bit more detail.

We have interviewed a number of activists who have been targeted, and use the insights gleaned from these interviews to draw some tentative conclusions about the capacity, motives, and techniques of Iranian hackers. We will also make a series of recommendations outlining how activists, civil society organisations, and tech companies can prevent and respond to these attacks.

BACKGROUND ON IRAN’S CYBER ARMY

While coordinated attacks on websites in Iran have been recorded as early as 2002, the 2009 post-election protests appear to have catalysed their efforts. One of the first major attacks that the Iranian Cyber Army took credit for involved defacing the Twitter homepage and taking the popular microblogging site offline for a few hours in December 2009.15

It was after the Stuxnet cyber attack on Iran’s nuclear infrastructure, which came to light in the summer of 2010, that the cyber army began to ramp up its activities. The following summer, an attack on Dutch certificate authority DigiNotar allowed hackers to monitor Iranian users connecting to Google on what appeared to be secure connections.17 It is difficult to definitively ascribe culpability for this attack, but available evidence strongly suggests the involvement of Iranian authorities. For example, stealing a Google certificate does not allow hackers to gain access to much information unless they control a fair amount of internet infrastructure (such as an ISP), which the Iranian government does. As the New York Times explains, “Armed with certificates stolen from companies like these, someone with control over an Internet service provider, like the Iranian authorities, could trick Internet users into thinking they were safely connected to a familiar site, while eavesdropping on their online activity.”18

Moreover, as a report on the incident from Dutch IT security firm Fox-IT notes, “The list of domains and the fact that 99% of the users are in Iran suggest that the objective of the hackers is to intercept private communications in Iran.”19

In addition to the attacks related to censorship and surveillance, there have also been attacks targeting the financial and military infrastructure of foreign countries, including the United States and Saudi Arabia, as well as businesses based abroad. As a comprehensive overview and detailed discussion of these attacks is beyond the scope of this report, we will instead provide a partial timeline. In December 2011, Iran claimed to have


16 Ibid


digitally hijacked an unmanned American drone flying along the border of Iran and Afghanistan (though this account is disputed by the US).

In August 2012, Saudi Arabia’s state-owned oil company Aramco was hit with a cyber attack that affected more than 30,000 computers (Iran’s Cyber Army didn’t claim credit, but circumstantial evidence points to Iranian hackers). During 2012 and 2013, the US accused Iran of launching cyber attacks against financial institutions, including Bank of America and PNC financial services group. And in 2014, Iranian hackers launched an attack on Sands, a Las Vegas casino owned by Sheldon Adelson.

**SPEAR-PHISHING ATTACKS**

Over the past two years, Iranian hackers have ramped up social engineering attacks aimed at civil society organisations. As a recent report from technology firm Check Point explains, “Since early 2014, an attacker group of Iranian origin has been actively targeting persons of interest by means of malware infection, supported by persistent ‘spear phishing’ [i.e. specifically targeted phishing] campaigns.” This cyber-espionage group was dubbed ‘Rocket Kitten,’ and remains active... with reported attacks as recent as October 2015."

An August 2015 report from Citizen Lab reached a similar conclusion, documenting a spear-phishing campaign targeting civil society groups which aimed to crack the two-step authentication process.

**INTERVIEWS**

To gain some insight into these attacks, we conducted interviews with two people familiar with the situation: Amir Rashidi, an internet freedom researcher at the International Campaign For Human Rights in Iran (ICHRI) who has done a lot of work with victims of attacks, and an Iranian human rights activist based in Europe who has been targeted (due to the sensitivity of the topic, we have kept the activist anonymous).

**HISTORY AND TECHNIQUES**

We asked Rashidi for his take on a range of topics related to Iran’s cyber army, including its history, capacity, preferred methods, and how civil society groups can respond. The following is a condensed summary of his remarks. Rashidi argues that Iran didn’t invest many resources in cyber operations until after the 2009 protests. Since then however, the government has poured a significant amount


of funding into developing cyber capabilities. And according to Rashidi, there has been some improvement in the Cyber Army’s capacity in recent years.

The Cyber Army’s hacking methods tend to not be particularly advanced. They often include social engineering techniques such as phishing, and targeted malware attacks aiming to deploy tools like keyloggers. These two approaches can be combined, as was the case in an attack described by Rashidi which aimed to deliver malware via email attachments designed to look like simple Microsoft Office (e.g. PowerPoint) files.

While these methods are not particularly advanced, Rashidi explains that they often serve their intended purpose of tricking activists or journalists into giving up sensitive information. He also pointed out that these attacks are rarely random. Instead, phishing emails are often crafted with an attentive eye towards the target’s interests and personal background.

CASE STUDY: TARGETING ACTIVISTS

This description of a careful crafted phishing email neatly fits the profile of the attack that targeted the activist we spoke to. As that activist told us, “The attackers seem to not only know me and my interests, but also constantly monitor my online activities and organise their attacks based on that.” The activist goes on to provide more specific details about the attack:

“Recently, I received an email from someone who pretended to be an officer [at a prominent human rights organisation] right after I had mentioned [that organisation’s] account in a few tweets. The sender—who impersonated a [member of that organisation’s staff]—sent me malwares [sic] in an email which looked ... very genuine.”

Such highly personalised targeting can make these phishing attempts quite difficult to spot. So how can activists defend themselves against these types of attacks? And how should they respond if they do fall for one?

FINDING SOLUTIONS

According to Rashidi, one of the best preventative measures activists can take is to familiarise themselves with basic cyber security practices, including topics like 2-step verification, avoiding attachments in emails from unknown senders, and encryption.

If an attack is successful, Rashidi stresses the importance of securing cooperation from tech companies like Facebook, Twitter, and Telegram in order to shut down a compromised account as soon as possible. This is an issue that Rashidi himself has been publicly involved with, when he recently lobbied Telegram to shutter the account of a BBC Persian journalist who had been arrested.26 This campaign ultimately succeeded in getting the account shut down, but it took nearly two weeks for Telegram to act, which was more than enough time for the attackers to download sensitive information and use the account for phishing attacks.

CONCLUSION

Based on the interviews we conducted with Rashidi and the activist who was targeted, we can draw the following tentative conclusions

about how Iran’s Cyber Army operates, and how civil society organisations can best defend against this threat.

The preferred method of Iran’s Cyber Army seems to be social engineering. In particular, Iranian hacking groups have become rather adept at crafting highly personalised and targeted phishing emails designed for various activists and civil society organisations. In short, Iran’s Cyber Army tends to use relatively unsophisticated techniques, but has become quite adept at specifically targeted social engineering attacks.

The best approach for civil society organisations defending against state-sponsored cyber threats is to combine preventative and reactive measures. In terms of prevention, basic cyber security training would prove very useful. In addition, a forum where Iranian activists and civil society organisations can share information about the threats they have faced might help raise community awareness about the common tactics, techniques and targets the Iran Cyber Army tends to pursue.

Reactive measures should include stronger collaboration between civil society organisations and tech companies like Facebook, Twitter, Google, and Telegram. When an account has been compromised, it is imperative that it is shut down as quickly as possible. In order for this to happen, coordination between activists and various tech companies needs to be streamlined, and set up in such a way that companies can quickly verify and carry out any takedown requests. As Iran’s Cyber Army improves its capacity to target activists, it is crucial that activists have the knowledge and resources to fight back.
May 2016 //
The Ongoing Impact of Tech Sanctions

In May’s report, we examined the impact that technology sanctions had on Iranian ICT users, and how these sanctions negatively impact the regular citizens’ abilities to carry out their rights.

Since the 1979 Revolution, the US has imposed various sanctions on Iran. However, the economic pressure on the Islamic Republic increased significantly during Ahmadinejad’s tenure, due to more wide ranging UN sanctions imposed in 2006, followed by several rounds of increasingly comprehensive EU sanctions beginning in 2010.

While the Iran nuclear agreement removed many of these sanctions, foreign banks and other companies have been reluctant to enter the Iranian market due to lingering fears of running afoul of the US sanctions against Iran that remain in place.27 This report looks briefly at the impact of these ongoing tech sanctions on Iranian users, and finds that they often serve to undermine freedom of expression, and inhibit the development of the Iranian tech sector.

THE HISTORY OF SANCTIONS

In addition to these wide-ranging measures, additional sanctions have been implemented to target ICT-related trade directly. In 1997, President Clinton signed an executive order prohibiting American individuals or companies from selling "any goods, technology, or services to Iran." This directive, notes Declan McCullah, "led to unintended consequences such as Utah-based Bluehost giving the boot to Iranian bloggers and opensource software site SourceForge.net denying access to Iranians." Over the past decade, foreign companies have imposed numerous restrictions on access for Iranians, likely due to the fear of violating a nebulous sanctions regime. In 2007, Yahoo and Microsoft removed Iran from their country lists, preventing Iranians from registering for Yahoo Mail and Outlook. More recently, Iranians have reported being unable to download apps from Apple's App Store. Hopes of liberalisation came in 2013 when the US lifted key high-tech sanctions against Iran, which resulted in Google Play finally becoming accessible in Iran (though only for free apps). But issues did not end there. In 2014, online education provider Coursera began blocking access to its online courses for students in Iran, Sudan, and Cuba due to confusion about whether or not they violated the sanctions against those countries. A discussion on a support forum on Coursera’s website suggests that Iranians are still struggling to access course materials and certificates in 2016.

So where does that leave us today? Which online services are available to Iranians and which ones are blocked? And how does lingering ambiguity about export controls affect Iranians at home and in the diaspora?

In order to attempt to engage with these questions, we sought input from three different sources. First, we conducted a survey of individuals living inside Iran, asking whether and how tech sanctions have impacted them in their daily life. We then asked two developers in Iran for their perspective, to get a sense of how these sanctions have impacted the tech industry in Iran. These individuals requested

anonymity due to the sensitivity of the topic. Finally, we asked two diaspora-based Iranian researchers for their perspectives—one foreign policy analyst, and one member of a civil society organisation—in order to see what ramifications these sanctions have outside of Iran.

OUR METHODOLOGY
Our approach to this research is meant to yield results that are indicative (rather than representative) of the impact tech sanctions have on Iranian users. The testimony and survey results discussed in this report are intended to offer a snapshot of a relatively small number of Iranians' attitudes, concerns, and reactions to tech sanctions, and should not be taken to represent the views of Iranians more generally.

SURVEYING OPINION
We sent out a short survey via a circumvention tools mailing list with over 200,000 subscribers asking respondents whether and in what ways they had been impacted by tech sanctions, receiving 403 responses. This survey is obviously not representative of Iranian internet users as a whole, but we think it provides a slightly broader view of the impact of tech sanctions than can be gleaned from the testimony of a few tech professionals. The results are presented and discussed below.

1) Have tech sanctions affected you in your day-to-day life?
   a. Yes 83.1%
   b. No 9%
   c. Not sure 7.9%

2) In what ways have tech sanctions against Iran affected you [mark all that apply]?34
   a. I have been blocked from accessing online services due to my country location (Iran). 78.3%
   b. I have had trouble advertising or selling services on online platforms 23.3%
   c. I have been unable to access online educational platforms such as Coursera or Edx. 28.6%
   d. I have had trouble purchasing web hosting services for a .ir website 18.7%
   e. I have been unable to use online payment services due to my country location. 67.6%
   f. Other [please specify]: 12.8%

Some responses:
- I cannot use many computer games and software because I live in Iran.
- I cannot download the latest versions of drivers for my OS.

Total responses: 433 individuals

A clear majority of respondents reported that they were affected by tech sanctions. Restrictions on online services appear to be the most common effect, impacting three quarters of respondents. This was followed closely by restrictions on online payment platforms, which affected around 67% of respondents.

Around 23% of respondents reported problems with advertising services online or accessing educational platforms, while just under 19% of respondents reported issues purchasing a .ir domain name.

34 If respondents answered “no” or “not sure” to question 1, they were instructed not to answer question 2.
IMPACT ON THE INDUSTRY
While sanctions have had some positive implications for Iran's tech sector - such as shielding Iranian companies from competition with global giants - they have also wrought havoc on the domestic ICT industry. Mahmoud Pargoo offers a tidy summary of the negative impacts of sanctions on Iran's tech scene:

“In relation to the supply chain, they made it difficult for manufacturers to purchase necessary components. Hence, manufacturers had to pay higher prices, with longer production lead times — which ultimately resulted in higher production costs. On the sales end, the sanctions caused a shrinking of exports and lack of interest in long-term contracts on the part of foreign companies. Furthermore, the high-tech sector was stripped of highly talented technicians — a trend that continues, notwithstanding the mild improvements during the past two years.”

So how do things stand today? Is any of this improving as a result of the nuclear agreement? To find out, we asked two Iranians working in the software development industry for their take on how sanctions affect the tech sector.

TESTIMONIAL #1 // AN IRANIAN WEB DEVELOPER
The main goal of the international sanctions was to target the government but it has had an impact on Iranians as well. For instance, various tech companies such as Google, Adobe, Bitbucket, and Nvidia have blocked Iranian IPs in order to prevent Iranians from using their services.

Hardware: With regard to hardware, some companies such as Nvidia and Advanced Micro Devices (AMD) have blocked Iranian IPs, which has prevented Iranians from downloading the latest version of drivers for their hardware. As a consequence, Iranians have been forced to use circumvention tools or VPNs to change their IPs in order to keep their software updated, or otherwise just settle for using outdated versions.

Software: Adobe and Google have both caused trouble for Iranians by obstructing their access to software, especially for ordinary users and developers. Because of tech sanctions, it has become nearly impossible for Iranians to use the latest technology such as Google Analytics, Google Firebase, and Android's documents and repositories. For instance, using Google Analytics’ Software Development Kit (SDK) and Google Code in an Android apps is meaningless, because when we go to check the results on Google Analytics we can only see a 403 error.


The error message displayed when Iranians try to visit developers.google.com

Also, some websites such as Adobe (Flash), and Oracle (MySQL)—which do not require any financial transactions—also block access to Iranians.

In the end, the tech sanctions imposed against Iranians have been more useful for the government, because they have kept Iranians away from the latest technology, and have prevented them from updating their devices. Thus, Iranian citizens are placed at a greater risk of hacks and surveillance, even putting aside the issues of internet censorship and slow connections.

It is interesting to note that this user reported issues with some of Google’s products, given that Google Play became available in Iran in 2013. There are a couple of reasons for this; in addition to Google’s server-side blocking (which poses a number of barriers to app development and tech support), users are unable to submit apps to Google Play without entering card details. This means that Iranians are dependent upon having someone based outside of Iran who can submit their apps using valid card details.

Moreover, the limitations on downloading updated drivers suggests that some Iranians will have to rely on outdated software, potentially exposing them to security vulnerabilities.

**TESTIMONIAL #2 // DIRECTOR OF APP DEVELOPMENT AT AN IRANIAN TECH COMPANY**

Iranians have suffered from Internet censorship by the government and also the “Reverse Censorship” by the Western companies due to international sanctions. Tech companies have blocked access to the majority of Google’s services, Oracle (especially downloads/updates of Java), Adobe, updates for anti-virus software such as Symantec, McAfee, AVG, Avast, and
ESET, along with Nvidia drivers, cPanel, some Microsoft services, and many more. This situation has forced users to download software updates from unofficial websites, which increases security risks.

These conditions became more complex and challenging for web and app developers because a range of fundamental app and web development services are blocked because of these sanctions. As a result, Iranian developers must use circumvention tools or VPNs to bypass these embargos. This might not seem like a big deal, but it creates serious issues because a developer requires access to a high-speed internet connection. The usual speed is 10 Mbps, which drops sharply to around 1 Mbps after connecting via circumvention tools, making it difficult for the developer to do their job properly.

It might be funny for the rest of the world but one of the main problems for big tech companies in Iran—with tens of millions of dollars worth of contracts—is finding good circumvention tools. Circumvention tools are a permanent fixture in their weekly meetings, even among company directors.

As a developer, these kinds of sanctions have forced me to give up some of my activities, which has caused me to lose part of my income. For example, the creative community website Envato made the decision to expand its operations from Australia to the US in 2015.37 As a result, this website has closed all accounts of Iranian freelance developers on all sub-services such as Themeforest and Codecanyon due to US sanctions. Many Iranian developers have lost their income as a result. Another example is the free software Android Studio. Despite this, developers cannot download content directly from Google—they have to download it from an Iranian clone website such as P30download. But this isn’t the end of the story, because sometimes we need access to a series of libraries which the software tries to download automatically, but which are blocked as a result of sanctions. Thus, the developers must download each library separately, which takes a lot of time. As a result, development time can be increased from an hour to a day or more. We also need to factor in the availability of circumvention tools and VPNs in our development timelines as well. Moreover, Android documentation, Google Console, and even Google Code Jam—which contains Iran in its country list—are not made available for Iranian IPs, and users must use circumvention tools in order to get access.

Also, Iranians cannot use .ir domains with some hosting companies, such as Hostmonster, Bluehost and Hostgator. Hostmonster removed 5-6 .ir domains from my panel without any notifications.

In conclusion, these tech sanctions have targeted private and freelance developers/companies because governmental organisations have more resources to circumvent them, for example by using special VPNs which use specific ports that remain accessible even when most VPN traffic is throttled. Also, it causes Iranians to believe that Western companies are opposed to them, restricting their access to services and platforms.

This contribution illustrates the issues tech sanctions can impose on the software development industry, including: restrictions on freelance work with American websites, difficulties acquiring development tools.

and challenges related to the accessibility of security software. In addition to echoing many of the concerns raised in testimonial #1, this contributor also highlights the challenges of registering .ir domain names, as well as the speed issues imposed by the constant requirement to use VPNs to acquire software updates and access to other forbidden services.

**TESTIMONIAL #3 // POLITICAL ANALYST NIMA RASHEDAN**

The tech sector in Iran was born out of tech sanctions and the lack of copyrights in the country. Most software on the Iranian market is pirated, and looking at the high level of mobile and internet penetration, it is not clear why people talk about the tech sector while other industries face bankruptcy as a result of the Iranian government’s policies. The tech sector is in a good place compared with other industries.

Also, the IRGC owns a big chunk of the tech sector in Iran [including a controlling stake in the Telecommunications Company of Iran—a major ISP and cellular operator]. The IRGC is on the terrorist list due to human rights violations and its activities in other countries in the region (including Syria). In the end, sanctions against the IRGC should be intensified in order to support and protect Iranian citizens. The government and the Iranian people must find a way to push the IRGC out of the market. Advanced technology in the hands of the IRGC is dangerous, and Iranians will be the first to suffer.

This contribution underlines an important point: the effects of tech sanctions on Iran’s IT sector are not exclusively negative. Indeed, one major benefit of the tech sanctions for Iranian tech companies is that they are shielded from having to compete with global giants like Google and Amazon, which has given the country’s nascent startup scene ample space to develop.

Rashedan also notes that the IRGC’s presence in the tech sector may serve to undermine human rights in Iran, and suggests that targeted sanctions should be intensified in order to drive the organisation out of the tech market. Although the IRGC’s role in the sector is worth noting, we would be somewhat more skeptical of the ability of additional tech sanctions to feasibly restrict the group’s online activities. Indeed, as previous contributors have noted, an intensification of tech sanctions is likely to have only negative impacts upon freedom of expression and digital security for Iranian developers and tech consumers.

Indeed, we would contend that tech sanctions have actually strengthened the position of state-backed and IRGC-affiliated initiatives by driving so many international competitors out of the market, and allowing state-linked companies to corner the market.

Tech Sanctions and the Iranian Diaspora

To get a sense of how tech sanctions impact Iranians living and working outside Iran, we spoke to Amir Rashidi, Internet Access Researcher at the International Campaign for Human Rights in Iran:

---


In recent years, there has been an increase in the Iranian users’ utilization of social networks with the aim of creating political and human rights-focused campaigns. Over the past two years, we witnessed users’ efforts to create ‘Twitter storms’ to this end. As an example, there was a Twitter storm to protest the Iranian government’s ban on stadium access for women. Unfortunately, because Twitter does not support geographic trends inside Iran, many of these activities are either never seen, or they are not as effective as the civil and human rights activists hope. Additionally, sanctions on technology also indirectly have an impact on Iranian users’ freedom of speech.

Because some of the tools the sanctions have banned for Iranian users are tools that would ensure their security, users feel unsafe carrying out their activities. For example, I received reports in some cases from users saying that they were barred from accessing applications such as Google Authenticator or Avast antivirus software. This leads to a loss of security and a fear of being identified which would indirectly impact the users’ freedom of expression. In one example, I was contacted by a reporter whose Google account had been hacked. After helping him to get his account back, I suggested he utilize two-stage identification, but unfortunately Google had blocked downloads of this application in Iran. As sending and receiving codes through text messages lacks security, I was able to install the application for him after a great deal of difficulty, just so he could work more securely.

Sanctions in the field of technology—particularly on financial channels used by these services—must be lifted. Although these sanctions have practically been lifted by the Iranian General

License D-1, many IT companies have refused to implement it. Even access to open source services in many cases remains banned for Iranian users. 40

A few points are worth noting here. First, Rashidi notes the often overlooked point that Twitter’s lack of support for geographic trends inside Iran limit the advocacy efforts of those using social media as a campaigning platform. Second, the blocks on the Google Authenticator app and Avast anti-virus software highlight the security risks that such sanctions can impose—however unintentionally—on Iranian internet users.

Twitter Reactions to #TechSanctions
In mid-2016, Iranian Twitter users have created a hashtag campaign to vent their grievances with implications of tech sanctions against Iranians: #فناتحريم (#TechSanctions). A number of tweets on this topic are listed below.

https://twitter.com/bkhzry/status/732437333098831872
Are they kidding us? I have checked with AsiaTech Internet! It’s not working again!
#TechSanctions
You try, too!

Behrouz Khezry
@behkhzry
شکیپک‌ن گرفته‌ای با اینترنت آسیا‌ترک چک کردم باید بله شده
که #فناتحريم
شما هم یا چک بکنید

A group of Iranian Twitter users have also banded together to create a comprehensive reference document showing the online services currently suffering from some form of sanctions-related service restrictions.

ICLab Censorship Measurement
We’ve heard from people who are impacted by tech sanctions recount their experiences. We’d now like to test how these sanctions are being implemented. With help from our friends at ICLab, we conducted an experiment testing whether a series of Western internet services (such as Google Analytics or Netflix) are accessible in Iran, using 4 different vantage points in the country.

In cases where the websites in question are not accessible, we’ve sought to determine whether the blocking was being implemented on the server side (i.e. by the companies themselves, likely due to sanctions) or by the Iranian authorities.

The table below illustrates the accessibility of each URL we tested, and if applicable, whether the blocking was implemented by the tech companies’ servers (“serverside”), or by the Iranian authorities (“local”). In our tests, we found that only Google was restricting access on their server side, although platforms such as Netflix and Bitbucket were being filtered by the Iranian government.
<table>
<thead>
<tr>
<th>URL</th>
<th>VPS-1</th>
<th>VPS-2</th>
<th>VPS-3</th>
<th>VPS-4</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://developers.google.com/">https://developers.google.com/</a></td>
<td>Serverside</td>
<td>Serverside</td>
<td>Serverside</td>
<td>Serverside</td>
</tr>
<tr>
<td><a href="https://get.adobe.com/flashplayer/">https://get.adobe.com/flashplayer/</a></td>
<td>Local (RST)</td>
<td>OK</td>
<td>OK</td>
<td>Local (RST)</td>
</tr>
<tr>
<td><a href="https://analytics.google.com/">https://analytics.google.com/</a></td>
<td>Serverside</td>
<td>Serverside</td>
<td>Serverside</td>
<td>Serverside</td>
</tr>
<tr>
<td><a href="https://code.google.com/codejam">https://code.google.com/codejam</a></td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td><a href="https://github.com/">https://github.com/</a></td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td><a href="https://azure.microsoft.com">https://azure.microsoft.com</a></td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td><a href="https://aws.amazon.com/ec2/">https://aws.amazon.com/ec2/</a></td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td><a href="https://www.dropbox.com/">https://www.dropbox.com/</a></td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td><a href="https://www.netflix.com/">https://www.netflix.com/</a></td>
<td>OK</td>
<td>Local (DNS)</td>
<td>Local (RST)</td>
<td>OK</td>
</tr>
<tr>
<td><a href="https://www.bitbucket.org">https://www.bitbucket.org</a></td>
<td>Local (RST)</td>
<td>Local (RST)</td>
<td>Local (RST)</td>
<td>Local (RST)</td>
</tr>
</tbody>
</table>

**NOTES:**

**RST** indicates that a website was blocked by the Iranian authorities via packet injection.

**DNS** indicates that a website was blocked by the Iranian authorities via DNS tampering.

Tests were conducted on 06/06/2016.

Refer to our April 2016 report for detailed descriptions of each of these methods.

---

Google

403. That’s an error.

Your client does not have permission to get URL / from this server. That’s all we know.

The page we were redirected to when we tried to access Google services from inside Iran.
CONCLUSION
While this report only offers a brief snapshot of the impact of sanctions, we think a few interesting results stand out. As this report was limited in scope and not intended to be representative, findings should be viewed as tentative indications rather than definitive conclusions.

It bears repeating that tech sanctions have produced benefits for Iran's tech industry, notably by shielding domestic tech companies from competition with global industry giants. In addition, the easing of sanctions following the implementation of the Iran deal has raised hopes of a more liberal climate for the accessibility of foreign internet services.

Yet it appears that despite the formal easing of sanctions, a number of restrictions still circumscribe the online freedoms of Iranian users. As we have seen, developers inside the country often struggle to access popular platforms like Google Analytics, whereas Iranians in the diaspora are prevented from using Facebook and Twitter ads to target users inside the country.

Such restrictions, it should be noted, constitute a series of de facto information controls that are layered on top of Iran's pervasive censorship system. Put another way, both the Iranian government and foreign tech companies restrict Iranians' access to information; the former as a matter of course and the latter due to attempts to comply with sanctions regulations.

While many of the issues discussed here are likely not intended consequences of sanctions, they nonetheless should begin to factor into the considerations of policy makers dealing with sanctions policy. In order to support the free flow of information in Iran, it is imperative that rules are clarified so that tech companies know where they stand vis-a-vis sanctions law, and that tech companies are willing to fight for their products and services to be accessible in Iran.
July 2016 // Public Data in Iran

July’s report looked at the accessibility of data released by the Iranian government, emphasising the need to facilitate greater access to these datasets through the increased development of infrastructure.

In the wake of the lifting of international sanctions on Iran, all eyes have turned to President Hassan Rouhani’s government to see if the President can deliver on his promises of rejuvenating the Iranian economy, stamping out corruption, and ushering in a new era of prosperity for Iran’s citizens. Against the backdrop of the continued economic influence of the Revolutionary Guard, and growing public anger at cronyism and financial corruption across the political spectrum, there is an urgent need to provide access to accurate, transparent public data relating to the country’s development.

We will set out the need to develop the data and statistical infrastructure of Iran, in order to facilitate greater public access to the datasets already published by Iranian authorities. By engaging in a series of short case studies, we will demonstrate that the volume of data already being released by government and state-affiliated departments is substantial, albeit rarely accessible in appropriate file formats, and generally obscured from public view.
THE OPEN DATA MOVEMENT

It is worth starting by offering a brief overview of ‘open data’ as a concept, and discussing the movement that has emerged around it. In the simplest terms, as described by the Open Data Institute (ODI), ‘open data is data that anyone can access, use and share’. More specifically, Open Knowledge International’s (OKI) Open Data Handbook notes that open data should fulfil three core principles, and should be:

- **Available and accessible**, at no more than a reasonable reproduction cost.
- **Reuseable and redistributable**, meaning that the license should permit reuse and redistribution.
- **Open to Universal Participation**, so that everyone must be able to use, re-use and re-distribute data, with no restrictions on usage.

The handbook goes on to note that such criteria are designed to ensure that interoperability is maximised, allowing diverse organisations, analysts, and systems to interact with the data. In order to develop truly insightful data analysis, or to develop effective products and services, different datasets must often be combined. Ensuring the interoperability of open data allows for a broad range of benefits, which we will now move to discuss.

THE OPPORTUNITIES OF OPEN DATA

Open government data furnishes a number of important benefits. As Kucera and Chlapek note, these include: (1) increasing government transparency, (2) enabling the government to better inform the public about its actions, and (3) allowing the government to improve its services. These benefits are discussed in greater detail below.

INCREASING GOVERNMENT TRANSPARENCY

Open data initiatives make governments more transparent by improving the availability and accessibility of data about public sector performance. This allows citizens to more accurately evaluate government policies, and hold elected officials to account more easily. A particularly clear example of open data’s role in facilitating greater transparency is the British platform ‘Where does my money go?’, which shows how taxpayers’ money is spent by the government. Users input their salary information into the site, and can see a clearly structured breakdown of where their tax is being allocated.

IMPROVE RELATIONSHIP BETWEEN CITIZENS AND GOVERNMENT

As stated above, opening up government datasets enables the public to better understand government actions, working to build trust and improve relations between

---


43 Ibid


citizens and their government. More specifically, as O’Hara argues, transparency and open data will be “damaging for unwarranted trust, but this will open up a space for warranted trust to flourish,” in that open data has the potential to puncture myths of governmental efficiency and good practice, but also allows for the government to boost trust by releasing information describing government achievements and processes accurately and completely.\textsuperscript{46}

An additional example of how open data can improve the relationship between citizens and government was visible upon launch of data.gov in the United States. Fung and Weil describe how “[the developers’] willingness to launch the site before all [the] data sets were identified, and to also enable users to openly rate the quality of the data on the site, are subtle but significant shifts in how government conducts information technology projects, moving away from control and perfection and towards iteration and interaction,” to draw users into the process of engaging with and co-creating datasets.\textsuperscript{47}

\textbf{IMPROVE GOVERNMENT SERVICES}

As Kucera and Chlapek explain, data about “public services can be analyzed and therefore its availability can help in identification of inefficiencies and subsequent improvement of the government services provision.”\textsuperscript{48}

2011 European Commission report entitled ‘The Pricing of Public Sector Information Study’ concluded that publishing data openly, and free-of-charge increased data reuse by 1,000 to 10,000 percent, attracted new users such as small and medium enterprises, and increased economic activity, market dynamism, innovation, employment and efficiency, with minimal impact on costs incurred by government.\textsuperscript{49}

\textbf{THE RISKS OF OPEN DATA}

Despite the benefits discussed above, open data projects can present dangers that must be kept in mind and mitigated as much as possible. In this section, we discuss some of the potential dangers and how we plan to address them.

Culture of secrecy in government

The publication of open data is sometimes perceived by governments as a high-risk policy that could threaten their legitimacy, and open them up to criticism. As Huijboom and Van den Broek note, “A crucial barrier for [open data policies’] implementation is the closed culture within government, which is caused by a general fear of the disclosure of government failures and any ensuing political escalation.”\textsuperscript{50}

This is a challenge particularly relevant to the Iranian context, as the government has in the past been accused of withholding or manipulating statistical information for political

---


reasons. The inherent challenges of developing expansive open data platforms in Iran with government support is another reason that Small Media has recognised the need to develop a platform independent of government oversight.

UNINTENDED CONSEQUENCES
The collection and publication of large data sets can sometime have unexpected adverse consequences on citizen behaviors. One example from the UK involves a program aiming to publish and map local crime data, which the Home Office argued would enable citizens to ‘hold their local police to account ... [by] pushing police to tackle crime’. However, a survey by insurance firm Direct Line found that since the announcement of the street-level crime map initiative, 11% of respondents decided not to report a crime they witnessed because they worried about the effect higher rates of crime mapping might have on house prices.

Commenting on this finding, professor of economic geography at the LSE Steve Gibbons noted that “the Direct Line survey suggests that detailed online crime data could have some serious unintended consequences, given the economic incentives for homeowners to conceal the true level of crime in their neighbourhood.”

When it comes to open data initiatives, emeritus professor of mathematics at Imperial College David Hand reminds us “that the very act of publishing the data will influence the quality of future data.”

It is crucial that engagement was large data sets is undertaken with due consideration given to potential consequences of publicising the data. Efforts to mitigate potential harm should be taken wherever possible, and considerations should be made of the potential impacts of releasing each dataset publicly.

ETHICAL CONSIDERATIONS
The publication of datasets entails ethical risks that are important to consider. In particular, it is imperative that steps are taken to protect the privacy of individuals whose personal information might be included in a large data set. Such considerations are clearly of high importance in Iran, where the consequences of the violation of privacy of certain individuals could result in the threat of arrest or imprisonment.

IRAN’S OPEN DATA LANDSCAPE
As stated previously, Iran already publishes large quantities of data publicly, however the platforms they use to do this are disparate, and are not standardised. It is often difficult to search for datasets, which are themselves

---


frequently incomplete or flawed, and in general the data and statistics infrastructure of Iranian government websites is deeply underdeveloped, and in need of investment and modernisation.

The following section will examine a number of online government data platforms in turn, to assess their strengths and weaknesses, and to identify the gaps in the field that necessitate the development of an independent open data platform for Iran.

**STATISTICAL CENTER OF IRAN**

The website of the Statistical Center of Iran

The Statistical Center of Iran (SCI) is a department of the Management and Planning Organisation of Iran, which is under the direct supervision of the Presidential Office. The SCI is the most credible website regarding statistics in Iran, and users are offered access to a vast range of online datasets (although some datasets have broken links).

The website is somewhat user-friendly, and allows users to explore a number of different categories such as financial markets, population, or industry and mining. In addition, each category is matched with a detailed description, helping users to develop their understanding of the data in each section.

Although the majority of datasets are in machine-readable .XLS or .CSV formats, some datasets have been published in .PDF format, which presents users with a number of challenges in terms of access and analysis.

For all its strengths, the SCI’s data frequently suffers in terms of availability and infrastructural reliability. For instance, the SCI was unavailable for non-Iranian IPs at the time of writing, likely owing to a June 2016 cyberattack on the website. As a consequence the SCI’s data was only available inside Iran, meaning that out-of-country researchers are forced to undertake convoluted methods to access the SCI.

Another challenge lies in the SCI’s lack of data from a variety of sources. Oftentimes, data published on the SCI will be contradicted by data published by other Iranian ministries or organisations. However, as these alternative datasets are not published on the SCI website, it is difficult to know what sources are available to compare and contrast with the SCI’s own data.
Another issue is the uncertainty around the continuity of the publication of some data. In early August 2016 the NOCR’s Director of Information and Demographics announced that the divorce rate would no longer be publicly announced, arguing that “publishing the data itself doesn’t solve any problems.” The day after, in a short announcement, the National Organisation for Civil Registration said the divorce rate will still be published.

The final issue regarding the NOCR relates to the volume of available data which has been published by this department. The available data on the NOCR website dates from 1383 (2004/5) and there is something of a black hole of information before this point. As a consequence, there is no official or reliable data available about births, deaths, marriages and divorces for roughly the first 25 years of the post-revolutionary period.
The website of the Ministry of Cooperatives, Labour, and Social Welfare

Another example of data being available in an inaccessible format is in the Ministry of Cooperatives, Labour, and Social Welfare’s (MCLSW) online registry of cooperatives. Although the website is difficult to navigate, and visually unappealing, users are able to search through the index of cooperatives registered with the MCLSW. There are a number of categories users can search by, including: province, name, keywords, or economic sector (agriculture, services, manufacturing, etc.). In the search results, up to 30 items are displayed at a time. By clicking on the name of a cooperative, a wide variety of details are available: the full name of the cooperative, a summary of its activities, the registration number, the province and city of registration, the registration date, the names and positions of board members, addresses and telephone numbers, their initial capital upon foundation, and their current capital, as well as gender breakdowns of the founding membership, and the current membership.

Evidently, the cooperatives register is a large and comprehensive database, but accessing its data is not a straightforward process, and filtering data to answer specific questions is impossible. For example, it is not possible to see how many cooperatives are registered in a particular year, or to know how many housing cooperatives were registered in a certain year in a certain province (unless the data is manually scraped).

The website of the Central Bank of Iran

The Central Bank of Iran (CBI) is the most powerful body in Iran’s banking system and one of the oldest state bodies in the country.
founded in August 1960. Despite its longevity and high profile, the CBI’s publicly available data has a number of issues we are eager to address.

A major issue in the CBI’s datasets is that of reliability in the face of political interventions and the manipulation of official statistics. Reports indicate that Mahmoud Ahmadinejad’s government put pressure on the CBI to refrain from publishing negative statistics about the government’s economic performance. Similar allegations have emerged about comparable interventions from the Rouhani administration, suggesting that the body is very susceptible to political pressure from the government of the day.

Additionally, the CBI’s datasets have frequently suffered from inconsistency in terms of structure, frequency, and availability. For instance, datasets concerning private sector property development are available between 1385 and 1394 (2006/07 to 2015/16), whereas the price index of consumer goods and services is available for a longer period, from 1381 to 1395 (2002/03 to 2016/17) although at some points data is for specific months rather than for entire years. Also, the CBI has failed to implement a common file standard for its datasets: some datasets are available in .XLS format, whereas many more are only obtainable in a comparatively cumbersome .PDF format.

The third and final problem with the site relates to the accessibility of data. This issues manifests itself in two distinct ways: a) Locating data is complicated, and requires the users to navigate through several levels of pages in order to navigate to the desired documents. Datasets are listed under 5 top-level categories, which are divided into a huge number of sub-categories. b) The data is not centralised, which means that users are frequently required to open a new website to find the data they need. For example, the Economic Time Series Database (ETSD) is available in a completely different site, which is itself challenging to locate on the CBI website.

CONCLUSION
As we have seen, the Iranian government and state-affiliated agencies already release a considerable volume of data. However, as the case studies illustrated, the datasets are often difficult to access, stored in obscure file formats, and generally hidden from public view. Digging through these datasets and converting them into usable file formats would help to facilitate greater public access to the datasets already published by Iranian authorities.

The concept of ‘Open Data’ assumes a certain level of interplay between the state and civil society, whereby the state makes the data on different aspects of its institutions ‘open’, so the civil society (and citizens) can utilise the data for different ends. Operationalisation of Open Data in a context such as Iran, where the state and civil society do not enjoy a trusted...
relationship, requires a redefinition. In such a context civil society has to accept a number of responsibilities that otherwise would have belonged to the state, in order to develop an open data ecosystem.

We would therefore note that civil society should play a leading role in the development of Iran’s data and statistical infrastructure, in order to facilitate greater government transparency, and create greater opportunities for data innovation and collaborative action.
August 2016 //
The National Internet: Up and Running?

In August’s report we took a closer look at the government’s implementation of its National Information Network.

Iran’s recent announcement of the completion of the first phase of its National Information Network (or SHOMA, to give it its Persian acronym) has generated a splash of publicity in the Western media. We’ll go beyond the headlines to offer an up-to-date overview of where the SHOMA network’s capabilities are at present, and highlight the potential risks (and benefits) that lie ahead for Iranian users.

Despite being in development for around a decade, the exact purpose and function of the SHOMA network remains somewhat obscured by conflicting government policy statements, which seem torn between characterising the network as service-focused, with the objective of granting users high-speed and low-cost internet access, and being security-minded, with the objective of protecting key government services from external cyberattacks.
SHOMA — A DECADE IN THE MAKING

While plans for a national information network were first sketched out as early as 2006, development was considerably accelerated in the following years owing to two major challenges to the Iranian political establishment. The first challenge was the post-election uprising in 2009. At the time, the only method the government had to stop protesters communicating online was to shut down the internet completely. Although the move helped the government to limit the organisational capacity of protesters, and severed their communications with the outside world, the sudden break created significant problems in that it also crippled infrastructure critical to the banking, transportation, and government sectors. This predicament highlighted the potential benefits of a National Information Network to host key services, as such a project would allow the government to temporarily cut off access to the global web while allow critical infrastructure to run on the domestic intranet.

In our March 2014 report, we put together an infographic describing the proposed structure of the SHOMA network’s infrastructure, showing the types of services that would be hosted on the network, and explaining how users would be able to connect to secure, SHOMA-based government sites through public eGovernment services (see Figure 1).

According to the latest official documents describing SHOMA - available on the Information Technology Organisation (ITO)’s website - the Rouhani’s government has undertaken some work to reshape SHOMA since 2014.

This new setup emphasizes SHOMA’s role in facilitating the flow of information domestically. The above graphic suggests a focus on the peering of data streams generated by various sources, including banking systems, content providers, and ISPs.

One of the crucial takeaways from this structure concerns the relationship between domestic SHOMA traffic and global traffic. Note that the peering point includes international traffic, as the references to Top Level Domains (TLD) and DNS root servers indicate, and the banking systems would need to connect to the global web as well. Based on what is suggested by this new structure, we can tentatively surmise that the government appears to be moving away from trying to permanently separate domestic and international traffic, at least in its public posture. However, it certainly remains possible that SHOMA will make it easier for the authorities to temporarily cut access to the global web during politically sensitive periods without harming critical infrastructure such as banking systems.

In addition to infrastructure, there is also the issue of security, which the 2010 Stuxnet cyber attacks brought to the fore of Iranian considerations. The Stuxnet cyber attack had a number of very serious impacts upon Iran’s energy infrastructure, causing centrifuges at...
SHOMA's intended structure, 2014
Iran’s uranium enrichment complex in Natanz to malfunction, and cause irreparable damage to themselves. As Kim Zetter notes, “Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment the computers controlled.”

The Stuxnet attack had a damaging impact upon Iran’s nuclear program, and in the process rattled Iranian authorities, underlining the importance of securing vital government and military networks to protect them from future cyber attacks and espionage. The Stuxnet attack may not have been a one-time incident, either: the 2016 discovery of malware in fire-stricken petrochemical plants raises a number of questions about Iran’s continued vulnerability to cyber espionage.

Iran’s uranium enrichment complex in Natanz to malfunction, and cause irreparable damage to themselves. As Kim Zetter notes, “Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment the computers controlled.”

The Stuxnet attack had a damaging impact upon Iran’s nuclear program, and in the process rattled Iranian authorities, underlining the importance of securing vital government and military networks to protect them from future cyber attacks and espionage. The Stuxnet attack may not have been a one-time incident, either: the 2016 discovery of malware in fire-stricken petrochemical plants raises a number of questions about Iran’s continued vulnerability to cyber espionage.

The combined threats of domestic unrest and foreign interference motivated Iranian authorities to accelerate the development of SHOMA, with authorities at the highest levels of government aggressively pushing the programme. In a September 2015 address, Iran’s Supreme Leader Ayatollah Ali Khamenei, Iran’s Supreme Leader called for Iranian authorities to launch SHOMA in order to protect itself against both cultural invasion from the West, and also ‘foreign intervention’ on the internet.

On August 28 2016 authorities finally announced that the first phase of development of the SHOMA network has been completed. But what does this actually mean for internet access in Iran?


71 Mahdieh Mohammadi, (2016), ‘We are not under pressure for filtering / We have to leave Telegram’, Mehr News Agency, retrieved 07/02/2017, http://bit.ly/2krbs9p
ADVANTAGES FOR USERS

Much of the media coverage surrounding SHOMA has focused on the negatives. While the introduction of SHOMA certainly does pose a number of serious risks to online privacy and freedom of information that certainly deserve careful consideration, the scale of infrastructure development taking place as part of SHOMA also promises some everyday benefits for end users that are frequently overlooked.

The most important publicly-stated benefit of SHOMA is that it provides reliable, high-speed connections for local websites and services such as banks, e-government services, and universities. In June 2016, Supreme Council of Cyberspace Secretary Seyed Abolhasan Firouzabadi announced that the price of internet subscriptions for users of Iran’s National Information Network (SHOMA) will drop to a quarter of its current price, while offering drastically higher speeds to end users.72

From initial reports it does appear that internet tariffs are indeed falling, suggesting that users may begin to see real improvements in the quality of their internet usage - at least for domestically hosted content. According to authorities, videos and other media hosted inside Iran would be accessed using the high-speed SHOMA network, making use of peering technology. Higher speeds and lower tariffs would allow lower-income Iranians from around the country to engage with the digital economy, and to access online content ranging from Aparat videos, through to online university courses and eGovernment sites.

DRAWBACKS FOR USERS

Notwithstanding the benefits discussed above, SHOMA entails serious risks to internet access and freedom of expression for Iranian citizens. The speed and cost incentives for businesses to host their websites inside Iran ultimately make domestically-hosted sites far more vulnerable to government intervention than those based outside the country, given the ease of access the government has to domestic data.

One recent example of a government-approved website shutdown is that of the news agency Memar News, which published a series of documents exposing corruption in Tehran’s municipal government. The Mayor of Tehran and the judiciary quickly intervened to shut the website down, and therefore silence the discussion around corruption.

Moreover, SHOMA could be said to violate net neutrality principles, as it only offers reliable, cheap, and fast access to the state-approved websites and services that are hosted inside the country. Such an arrangement, coupled with censorship of some foreign websites, will likely give users incentives to opt for local alternatives, which have had their content strictly controlled and regulated.73 In the long run, this ‘nudging’ of users towards easily accessible domestic content could amount to a ‘soft censorship’, in that it disincentivises users from gaining access to foreign-hosted content that could contravene Iranian law.

The increasing registration requirements for Iranian users of SHOMA pose another threat to user security. Under existing plans, users are required to register their IP address alongside


their national ID number and home address, as a prerequisite for ISPs and mobile networks to provide internet access. As a consequence, the government will swiftly be able to identify users of SHOMA who attempt to access content deemed problematic for Iranian authorities.

**SHOMA AND THE GLOBAL WEB**

While there has been some speculation that the launch of SHOMA might lead to Iran being cut off from the global internet, we don’t think this is a likely outcome, primarily because many services and businesses in the country are completely dependent on the internet. The best example lies in Iran’s startup ecosystem, which is completely dependent upon international services such as Google products, Mailchimp, Zendesk, and a massive array of design and development software in product development. Cutting off global internet access permanently would destroy the startup sector in an instant. Cutting off global internet access would likely be an incredibly unpopular move even among many on the right-wing of the Iranian establishment, as platforms such as Instagram and Telegram have also been utilised by conservatives to try and promote their own political agenda.

A more likely issue concerns temporary internet shutdowns during politically sensitive periods, such as elections. The Iranian government has shown a proclivity towards shutdowns in the past (it throttled speeds dramatically in 2013), and the launch of SHOMA considerably lowers the cost of doing so in the future, insulating critical governmental, banking, transportation, and other core infrastructure from the negative effects of an internet shutdown.

Recent Developments and Conclusions

This all being said, it’s still somewhat unclear exactly what has changed since the government unveiled SHOMA at its launch event in August. Users have reported no significant transformation in their online experience, and very little appears to have changed in reality. So why all the fanfare?

One possible explanation is that the Rouhani government needed to put on a show for hardliners to demonstrate that ‘progress’ was being made in the implementation of SHOMA. Hardliners on Iran’s filtering committee, and in the Supreme Council of Cyberspace have castigated Rouhani’s government for dragging its heels on the development and implementation of SHOMA, and this launch event may go some way towards appeasing these elements in the establishment.

It is also worth bearing in mind that this ‘launch’ event was only for the first phase of SHOMA - not the full network. Many of the promises made by the government about Phase I relate to infrastructure development, security systems, and other behind-the-scenes type work. The objectives for Phase I’s launch are listed below:

---

The vagueness of these promises is notable. ‘Increased security’ and ‘increased development of local content’ are very flexible as goals, as is the ‘provision of different kinds of digital services’. Our previous reports have shown that the government is investing in infrastructure development, and appears to be making efforts to drive content hosting into the domestic sphere, but these are incremental processes. The grand ‘Phase I’ launch event held in August demonstrated nothing new, and very little of substance.

In addition, since the publication of these launch objectives, the government has made a number of statements about the impact of the Phase II rollout upon users, and the structure of Iran’s internet more broadly. The government has announced that users will receive 50% off on their domestic data tariffs, meaning cheaper internet access for those using domestic services.  

More worryingly, the government has also stated that the rollout of Phase II would see regional data centres developing the capacity to divide domestic traffic from international traffic. On December 28 the Communications Regulatory Authority (CRA) ordered all Iranian ISPs to operator to divide their domestic traffic from International traffic by January 20 2017. According to the CRA this measure would help to decrease user internet tariffs,  


though we would note that it could also allow the government to easily cut Iran off from the global internet in times of political instability without affecting a number of core, domestically-hosted local services. As of early February 2017, it is as yet unclear how this development will impact upon users’ experiences online.

It is of crucial importance to monitor the ongoing development of SHOMA, and the implications of the existing system for user privacy and freedom of information are deeply troubling. But the ‘launch’ of Phase I of SHOMA did not appear to mark the beginning of a new era in Iranian internet censorship. Iran’s systems and methods of information control continue to evolve in a problematic direction, but they do so incrementally, and at a generally slow pace.

If the launch of Phase II in February 2017 has indeed resulted in a separation of domestic and global traffic, then there is cause for concern. Small Media will continue to monitor the development of SHOMA throughout 2017, and report on any incidences in which it facilitates the strengthening of Iranian state information controls.

| PHASE III  
NETWORK COMPLETION  
MAY 2017 |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The full realization of a functionally independent, and content-populated network, with secure infrastructure and services to protect users and their privacy.</td>
</tr>
<tr>
<td>Further creation of domestic content and products, including high-speed domestic broadband for the private sector.</td>
</tr>
<tr>
<td>The prioritisation of domestic traffic over international traffic.</td>
</tr>
<tr>
<td>Development of ICT in the private sector.</td>
</tr>
<tr>
<td>The creation of new e-services for the public, including online shopping and banking services.</td>
</tr>
<tr>
<td>Further development of e-Government services.</td>
</tr>
</tbody>
</table>
In 2014, Small Media published a trio of reports about Iran’s startup ecosystem, aiming to separate the facts from the fiction, and to cut through the hype around Iran’s nascent tech sector. This feature from October 2016 reviewed the situation facing Iranian startups in the post-nuclear deal landscape, assessed recent policy shifts, and made a number of predictions about the future prospects for the sector at the end of Rouhani’s first term.

EXISTING CHALLENGES
In November 2014, Small Media identified four major challenges faced by Iranian tech entrepreneurs that serve as obstacles to the development of their businesses:

1. Poor infrastructure
2. International sanctions
3. Lack of investment
4. Internet censorship

Interestingly, on the first three challenges, the Iranian government has been moving in a direction that supports the development of the country’s startup sector.

INFRASTRUCTURE DEVELOPMENT
The country’s internet infrastructure has seen marked improvements since our last report in 2014. According to statistics published by Iran’s ICT Ministry in September 2016, Iran’s internet bandwidth increased from 130 Gbps in March 2014 to 564 Gbps in June 2016.\(^7_8\)

Rural internet access is also on the increase, with the total number of internet-connected villages increasing from 52,000 in March 2013 to around 55,000 by June 2016.

Also worth noting is the emergence of government-operated advice centres for investors, entrepreneurs, and local ICT suppliers, under the umbrella of the National Network for the Technology Market (NNTM). These offices are being set up in Iran’s ever-expanding technology parks, including the flagship Pardis Technology Park on the outskirts of Tehran, and are demonstrative of the government’s continued enthusiasm for the national boom in tech startups.

The government is steadily increasing the capacity and reach of its network infrastructure, and is investing in other support systems to inject greater vitality into Iran’s tech startup sector.

SANCTIONS AND FOREIGN INVESTMENT
The lifting of international sanctions on Iran in January 2016 stoked expectations of a gold rush among Iranian tech leaders, who sensed a golden opportunity for Iran’s nascent tech sector to attract big bucks from global investors (Tech in Asia and the Jerusalem Post posted pieces that rode this early wave of optimism).\(^7_9\)

Although significant obstacles still remain (as we’ll explain later), foreign investors have been beginning to explore opportunities in Iran’s startup sector. In 2016, the Iran Industrial Development Investment Company sold 7.83% of its shares in Sarava Pars (the holding company for startup giants Cafe Bazaar and Digikala) to a Swedish company for 6.4 million Euros.

State investors are also eyeing up tech opportunities in Iran. Wang Zhan, President of the Shanghai Academy of Social Sciences announced in June 2016 that Chinese companies would be investing in the future development of the Pardis Technology Park. ICT Minister Mahmoud Vaezi’s September 2016 charm offensive to Sweden and Finland also resulted in some tentative agreements about future collaboration in the areas of technology and scientific development.

That said, ongoing security risks and regulatory challenges have meant that foreign investors have been relatively slow to buy into the hype around Iran’s startup sector. Despite growing infrastructure investment and the removal of international sanctions, the outlook for Iranian startups remains troubled.

ONGOING CHALLENGES
Although as noted above, the Iranian government is making some progress in developing the country’s network infrastructure and removing the barriers of international

---


sanctions, deep-rooted challenges remain. Regulations around digital businesses are incredibly burdensome, trust in government policy is low, and the Iranian Revolutionary Guard Corps continues to perceive the tech sector as a ‘trojan horse’ for foreign influence – many rising entrepreneurs have suffered dearly as a result.

In the following segment we track the ongoing challenges still faced by Iranian tech startups, and note how they might be overcome through processes of reform or other forms of governmental engagement.

**REGULATORY FAILINGS**

The existing regulatory frameworks governing the existence of Iran’s startup sector are sprawling and threaten to strangle off growth of young tech companies. Many of these challenges relate to commercial licensing requirements, although censorship and content licensing are also limiting the ability of digital content distributors to work effectively.

The Iranian government requires all websites engaging in financial transactions to register with the eNamad database, which we discussed in our May 2014 report. However, in order to receive an eNamad license companies must prove that they meet 38 regulatory requirements, including property ownership or financial guarantors – a tall order for young entrepreneurial Iranians who lack start-up capital, connections, or a home to call their own (see our May 2014 report for more details on regulatory requirements). Companies selling software, digital media (music, ebooks, films, etc.) and other digital goods are also required to receive permission for each item from the Ministry of Culture and Islamic Guidance. Such requirements are an onerous burden for many small start-ups operating with limited human and financial resources.

These challenges are not new – Small Media highlighted the challenge of overregulation in its November 2014 report. To illustrate the ongoing challenges that arise from regulatory failings, we can present two examples of banking and finance-focused startups that have been negatively affected by overregulation.

**Bahamta** was a web-, iOS-, and Android-based payment system that helped Iranians to issue invoices and process online payments. Although it is unclear exactly how many people used Bahamta, Google Play statistics show that the Android app was downloaded at least 1,000 times.

Two years after launching, Bahamta published a blog post on 3 September 2016 announcing that it was ceasing operations and closing down its numerous platforms. According to this blog post, Iran’s Electronic Payment Card Network (or SHAPARAK) – which is under control of the Central Bank of Iran (CBI) – asked Bahamta to cease operations in Spring 2016, as it was not registered with eNamad.

After receiving this notice, Bahamta tried to convince SHAPARAK that for a startup to cease operations is as good as a death sentence, and stated that it was unable to meet eNamad’s tough obligations on property ownership and financial guarantors. Instead, the company offered to move forward and follow all the regulations it was able to, while assisting SHAPARAK to update its regulatory frameworks

into a form more suited for a 21st century economy.

According to Bahamta, a letter was sent to SHAPARAK on May 17 detailing these challenges. The company received a response on June 7, stating that SHAPARAK will disable all of Bahamta’s payment gateways.

In a long blog post, Bahamta responded to SHAPARAK’s letter and answered its points in turn. In summary, the post stated that the main issue that forced Bahamta to close relates to a lack of appropriate and effective regulation around online banking, and the lack of creative approaches to the management of Iran’s financial sector.

PayPing is an Iranian analogue of Paypal that faced very similar challenges dealing with SHAPRAK. On August 30 2016, PayPing announced in a blog post that its services would cease temporarily while awaiting an eNamad license. In this post, PayPing complained about Iranian authorities’ attitude towards startups, stating: “Unfortunately, on the one hand [Iranian] authorities have encouraged [Iranian] entrepreneurs to go out and [launch] financial startups, but once they’ve had time to grow they’re ordered to shut down because they lack the correct eNamad registration.”

EXISTING MONOPOLIES
Another major obstacle which may prove very challenging to overcome in the short term is the dominance of monopolies in Iran - especially in the ICT sector. Small Media has previously reported on the commanding influence of the Telecommunication Infrastructure Company (TIC) over the management of internet bandwidth inside Iran.82

The startup ecosystem is similarly at the mercy of existing monopolies, with a number of companies having already been muscled out of business by bigger beasts in the sector. The most recent example relates to a number of Android apps developed for Aparat, the popular Iranian video sharing platform. On 17 October 2016, all of Aparat's affiliated Android apps were removed from the popular app store Cafe Bazaar, including Aparat, Aparat Kids and Filimio.83

According to Hessam Armandehi, CEO of Cafe Bazaar, his company was forced to remove these apps as the result of an order from Iran's Court for Culture and Media (ICCM), after the state broadcaster IRIB claimed that Aparat was hosting IRIB content, thereby breaching copyright. At the time of writing, all of Aparat's apps remain unavailable on Cafe Bazaar.

This example demonstrates the dangerous situation facing startups that threaten the status quo inside Iran. Aparat is a huge player in Iran's tech market, and has received enthusiastic backing from government officials in the past. That the IRIB felt threatened enough to wage war against the platform speaks sends a clear message about the willingness of old power structures to do everything in their power to stave off younger challengers in the startup sector.

SECURITY RISKS
The domestic politics of Iran have always made it a high-risk market for investors and entrepreneurs, and the signing of the nuclear deal has only been able to have a limited impact upon mitigating the dangers of investing in the country. Many stakeholders in the Iranian political and intelligence establishment retain hostile attitudes towards foreign engagement and influence, and a paranoia around Iranian dual nationals who would like to work and invest in Iran.

In recent years, there have been numerous examples of entrepreneurs who have been arrested by Iranian intelligence services as a result of their receiving funding or support from foreign sources. Arash Zad is a prominent entrepreneur who lived in Istanbul while establishing a number of innovative online services. Zad was arrested in August 2015 as he was attempting to travel back to Turkey after a trip to Iran.\(^{84}\) Kamran Ghaderi, the director of the Vienna-based ICT company Avanak was arrested when he travelled to Iran with a group of Austrian businessmen and women in 2015, and was subsequently sentenced to ten years in prison.\(^{85}\) Even foreign nationals are at risk of detention: in 2016 the Lebanese businessman Nizar Zakka was sentenced to ten years imprisonment, and ordered to pay a fine amounting to 4 million USD.\(^{86}\)

These kind of cases have understandably made investors nervous about engaging in activities inside Iran, as they are unable to receive even any basic guarantees about the safety of their financial investments or personal safety. At the same time, Iranian entrepreneurs have been placed in an awkward situation that means they risk investigation, fines, and even imprisonment if they seek sources of foreign investment and funding to develop their businesses.

This crackdown on foreign investment has been part of a concerted strategy of hardline politicians, and officials aligned closely with the Islamic Revolutionary Guard Corps (IRGC). Over recent years, they have attempted to portray Iran’s startup sector as part of a Western project of infiltration, even going as far to produce a documentary about the subject, named ‘Shabnameh’.

Shabnameh is a documentary produced by Safir Film, and directed by Seyed Mehdi Karbassi - a graduate student from Sharif University of Technology. Shabnameh tells a story based on the relationship between Iranian startups and foreign powers (most


prominently the United States). In an interview with state broadcaster IRIB, Karbassi said that he made this documentary to highlight the perceived risks of foreign infiltration and espionage through foreign investment. In an interview with state broadcaster IRIB, Karbassi said that he made this documentary to highlight the perceived risks of foreign infiltration and espionage through foreign investment.87

The Shabnameh trailer shows that authorities have granted access for the filmmakers to interview Siamak Namazi, who was sentenced to ten years in prison due to ‘collaboration’ with the US government. At the time of writing this documentary has not been broadcast for a mass audience, although a number of private viewings have been undertaken at universities. Meanwhile, hardline conservative politicians have been promoting Shabnameh publicly, and have cited the film as evidence of the relationship between Iranian tech startups and Western ‘infiltration projects’ in Iran.88

In such an atmosphere of paranoia and hostility towards foreign investment, many donors and investors are understandably nervous about engaging enthusiastically with Iranian entrepreneurs, and until the challenge of this toxic environment is resolved, it will remain challenging for young Iranian tech leaders to truly engage fully with global markets.

**SURVEILLANCE FEARS**

As a consequence of widespread state surveillance of digital media, many Iranians feel a sense of unease around using apps that could easily be monitored by state authorities – namely, those hosted on domestically located servers. For instance, according to an online poll conducted by Nima Akbarpour – the presenter of BBC Persian’s technology show ‘Click’ – 71% of Iranians would stop using the messaging app Telegram if it relocates its servers to Iran.89

This lack of trust can massively cost Iranian startups, and prevent them from effectively scaling up or significantly expanding their user base. In order to grant tech startups the space to attract trust and loyalty from domestic users, the Iranian government should thoroughly reexamine its policies relating to surveillance and censorship, and refrain from

**CONCLUSION**

Iran remains an intensely challenging country for tech entrepreneurs and investors, owing to a continually hostile intelligence and security establishment, byzantine, contradictory and constricting regulatory structures, and aggressive monopolistic organisations that fail to tolerate marketplace diversity.

That being said, the current Iranian administration has demonstrated clear intent to support the development of the tech sector, investing significantly in network infrastructure, technology centres, and entrepreneurial support mechanisms such as the NNTM. But if the government truly wants to take advantages of the economic opportunities offered by the nuclear deal, it must move to simplify and clarify regulatory structures, break up monopolistic organisations, and bring the security establishment to heel. Of course this

89 Akbarpour, N. [@nima], ‘If Telegram servers move inside Iran…’, Twitter, 16/08/2016, retrieved 07/02/2017, https://twitter.com/nima/status/765478626733228032
is no easy prospect, but the possible benefits of unlocking the potential of Iran’s young, innovative, entrepreneurs are enormous.
The Big Picture

In the following chapter, we provide a comprehensive overview of key policy developments from 2016 in three important policy areas: the government’s relationship with Telegram, its development of the ‘National Internet’ (or SHOMA), and the government’s push to develop domestic online services.

We catalogue policy developments comprehensively, and on a monthly basis. For all our latest documentation of Iranian internet policy developments, be sure to follow our work in 2017 at smallmedia.org.uk/work/filterwatch.
Over the course of 2016, there were a series of long-running battles between state officials over the status of Telegram, the most widely used messaging app in Iran. Whereas Rouhani’s ICT Ministry has generally taken a flexible position on permitting Telegram to operate, in the latter part of the year it began to back calls for the registration of Telegram channel administrators with the government.

The Rouhani government has notably held firm in the face of critics on the Filtering Committee (CDICC) who have called for Telegram to be banned completely. But there are also a number of questions that have arisen about Telegram’s relationship with the Iranian government, and its willingness to accede to government demands in order to preserve its market dominance. Read on for the full story.
January 1: According to the Iranian Students’ Polling Centre (ISPA), 53% of Iranians use social networks, and Telegram has 20 million users in Iran. The key survey findings are listed below:

- 72% of 18-29 year olds are members of at least one social network. This figure narrows to 53% among 30-49 year olds, and to 25% of over-50s.
- 67% of Iranians said they are members of comedy-sharing groups, 46% are in science-focused groups, 38% in news and politics-focused groups, 26% in family-related groups, 16% in sport-focused groups, and 15% for cooking groups, 14% religious groups and 7% for sexuality-related groups.
- 38% of respondents said that social media is a positive phenomenon, 23% described it as negative, and 31% refused to comment.
- Of respondents who reported membership of at least one social media platform, 55% responded that social media is a positive phenomenon, 9% described it negatively, and 33% refused to comment.
- 55% of men and 51% of women are users of at least one social network.
- 75% of university-educated respondents are members of at least one social network.
- 39% of respondents with a high school diploma or less are members of at least one social network. (Source)
Iran’s ICT Minister Mahmood Vaezi kicked off 2016 on a hopeful note by insisting that the government had no plans to block Telegram, and that its much-vaunted ‘Intelligent Filtering’ system would suffice for the purposes of filtering problematic content on the platform.90 Interestingly, on January 13 Vaezi claimed that Telegram would comply with any Iranian requests to close channels that operate ‘in violation of Iranian law’.91

In a direct and pointed rebuff to Vaezi, Abdolsamad Khoramabadi, head of Iran’s CDICC, emphasised the judiciary’s authority to block any applications or social networks that operated in violation of the law.92

**FEBRUARY**

February saw the emergence of a new critique of Telegram with Supreme Council of Cyberspace (SCC) member Seyed Mohammad Reza Aghamiri proposing that it should move its servers to Iran, or be filtered.93 This marks the beginning of a concerted push by Iranian authorities from a variety of institutions to nudge Telegram towards relocating some of its operations to Iran, thereby making public communications more susceptible to state surveillance and shutdowns.

Elsewhere, there were some reassuring signals from the head of the SCC that the filtering of the messaging app was not seriously being considered by authorities. Seyed Abolhasan Firouzabadi noted that to filter Telegram would be a futile gesture, as every time a platform is filtered Iranian users simply migrate to a

---


new one. He noted explicitly that the rise of Telegram in Iran only came after the blocking of Viber, and that the only long-term solution involves the development of domestically produced messaging apps. Iran’s Minister of Culture and Islamic Guidance Ali Jannati also spoke out against the blocking of Telegram and WhatsApp.

Despite the ongoing debate around the status of Telegram during the February 2016 parliamentary elections, no major service disruptions were reported.

MARCH

March in Iran coincides with the Persian New Year holiday. The month always sees a lull in public announcements, and this year was no different. No new policy initiatives were announced relating to Telegram in March, though the head of Iran’s Cyber Police (FATA) Seyed Kamal Hadianfard did report that 460 ‘campaigning violations’ took place over the course of the campaign period, adding that an (unspecified) majority of these took place on Telegram. Alireza Azarderakhsh, Head of the Cybercrime Prevention Department at FATA, added that Telegram was being used to share a number of tools and tutorials designed to help people engage in cybercrime. No examples or further details were provided, and FATA did not unveil any additional measures it would take against Telegram or Telegram users.

APRIL

April saw Iran make claims of additional cooperation with Telegram over the blocking of pornographic channels on the platform. On April 3, Press TV reported that Telegram had blocked 50 pornography channels in a 48 hour period. Vaezi added on April 12 that Telegram would close pornographic channels within 24 hours of a request by Iranian authorities.

MAY

May saw Telegram being blamed for a number of ills on the Iranian web, from cybercrime to sluggish internet speeds. FATA Chief Seyed Kamal Hadianfard claimed that 35% of all reported cybercrimes in 2016/17 had taken place on Telegram, whereas former ICT Minister Reza Taghipour claimed that up to 40% of Iran’s international internet bandwidth was being used by Telegram (thereby slowing down Iranian access to global web content).

Interestingly, Vaezi also restated his government’s close working relationship with Telegram, stating that it was cooperating to block objectionable content flagged up by the
ICT Ministry. The seemingly cosy relationship between the Rouhani administration and certain social media platforms was raised by a conservative MP Nasrollah Pejmanfar, who accused the government of being soft on social media platforms because they obtain political advantages from them.

JULY
Telegram’s Iranian operations were rocked in July by the publication of the personal details of more than 20 million Irancell customers. Although MTNBotPro (the bot responsible for spreading the information on Telegram) was rapidly blocked, the incident played into Iranian authorities’ characterisation of Telegram as a hotbed of criminal activity. FATA Chief Hadianfar warned users against using Telegram while its servers were located outside of Iran, stating that foreign governments would be able to exploit user data at will.

AUGUST
Conservative and hardline critics of Telegram were particularly active in August. CDICC Secretary Abdolsamad Khorramabadi called Telegram harmful, and insisted that Iranian officials should follow up and provide support to domestic messaging applications so that Iran could one day ‘say goodbye’ to Telegram for good. Grand Ayatollah Naser Makarem Shirazi also noted that the network bandwidth that has been allocated for the use of Telegram should be ‘redirected’ into SHOMA, and that efforts should be made to develop similar apps domestically.

Although it is hardly out of the ordinary for hardline clerics to make such statements, August does mark the point at which Vaezi himself begins to take a harder line on Telegram, stating on August 21 that the government had not yet made a final decision over whether or not to censor the platform, and noting on August 23 that Telegram should not be permitted to operate inside Iran unless it relocates its servers there. This hardening of his tone marks a departure from his previous laissez-faire position on Telegram’s activities.

SEPTEMBER
After a tough August, September saw the government’s position on Telegram mellow once more. No longer threatening it with censorship, Vaezi instead justified his position by stating that the censorship of online social media platforms is futile, as users will always simply migrate to different ones. Instead, he argued, domestic platforms

should be developed to entice users away from international alternatives like Telegram,\textsuperscript{107} an argument supported by SCC Secretary Firouzabadi.\textsuperscript{108}

A controversy also emerged over the use of Telegram to communicate in an official capacity within government departments. Although Vaezi insisted that action would be taken against government departments found to be using the app, he stated he was unaware of the app being used in a systematic manner. This is an interesting criticism considering the ICT Ministry has an official Telegram channel: telegram.me/ictministry.\textsuperscript{109}

\textbf{OCTOBER} \\
A quiet month. CDICC Secretary Khoramabadi - usually a very outspoken critic of Telegram - denied reports that the messaging app would be blocked in order to force Iranian to migrate to domestic alternatives.\textsuperscript{110}

\textbf{NOVEMBER} \\
Another relatively uneventful month with regard to Telegram. Speaking at the Press Exhibition, SCC Secretary Seyed Abolhasan Firouzabadi stated that the government would soon make a decision regarding mandating the relocation of Telegram servers to Iran,\textsuperscript{111} but no further actions were taken.

\textbf{DECEMBER} \\
As 2016 ended, the debate around Telegram shifted. Dr. Aliasghar Amidian, Director of Iran’s Communications Regulatory Authority (CRA) stated that if Telegram operates in compliance with Iranian law and regulations, then it would not be required to establish local servers within the country.

Instead, a number of different officials announced that a new registration scheme would be launched to collect the details of all Telegram channel administrators managing channels with more than 5,000 users. Vaezi announced that channel administrators must register with the Ministry of Culture and Islamic Guidance (MCIG) and obtain a license in order to continue managing their channels legally.\textsuperscript{112} This was later confirmed by both FATA Chief Hadianfar and the MCIG’s Deputy Minister for Digital Media Mostafa Ashraf.\textsuperscript{113} Critics of the initiative noted that it would be very difficult to ensure that Telegram administrators actually step forward to identify their details, although SCC Chairman Firouzabadi insisted that

\begin{thebibliography}{9}
\bibitem{112}ITNA, (2016), ‘Mr. Minister! Well done, but what are you doing with ‘proxy media outlets’?’, retrieved 07/02/2017, http://news.parseek.com/Url/?id=13312932
\end{thebibliography}
measures were being put in place to ensure that this occurs.\textsuperscript{114}

The registration site launched on the website of the MCIG’s Information Technology and Digital Media Centre (SARAMAD) in mid-December,\textsuperscript{115} though no statistics are yet available as to the number of registrations that have taken place.

**CONCLUDING OBSERVATIONS**

So despite being at the top of ICT policymakers’ agenda throughout 2016, Telegram emerged from the year generally unscathed. Support from officials in the ICT Ministry, SCC, and MCIG was vocal enough to fend off harsher critics within Iran’s Filtering Committee, and talk about mandating relocation of servers to Iran was just that - talk. That said, the recent introduction of registration requirements for Telegram administrators is troubling, although at this point we would note that enforcement of the system looks to be near-impossible.

Despite the high-profile conflicts over its status, Telegram usage in Iran is still growing. Iran’s Cyberspace Research Institute published the findings of a new research project, finding that around 170,000 Persian-language Telegram channels are currently in existence, and more than 11,000 have over 5,000 members. More than 1.5 million items of content are published each day. The average Iranian Telegram user is a member of 13 Telegram groups, and views around 100 items of content on a daily basis.\textsuperscript{116}

At this point Telegram is firmly rooted in Iran’s digital landscape, and appears to be there to stay. The continued resilience of the app makes it all the more important to continue asking questions about the security of the platform, and ongoing claims about its complicity in government censorship efforts. Telegram is undoubtedly an incredibly influential media platform in Iran, but until these concerns are satisfactorily allayed it remains a risky environment for political activists and human rights defenders to operate within.


\textsuperscript{116} Mehr News, (2016), ‘There are 11,000 Telegram channels with more than 5,000 members’, retrieved 07/02/2017, http://bit.ly/2kAyLOS
The Big Picture //
SHOMA

Unsurprisingly, Iran’s National Internet (SHOMA) proved a hot topic for 2016. Despite repeated criticisms of the project for massively overrunning in terms of its timeline and budget, the first phase of the network was finally rolled out at the end of August, and the second phase pushed publicly in February 2017.

As discussed in our August 2016 feature, the architecture and function of SHOMA seems to have undergone a number of radical revisions since its first conception in 2006, and is unlikely to act as an entirely self-contained network that will sever Iran from the global internet (as was the fear of some global commentators during the Ahmadinejad administration). Nonetheless, the battles and debates over SHOMA in 2016 have demonstrated that the Iranian establishment still sees the high-speed network as a means of weaning citizens off global online content, while establishing a number of new mechanisms for internet controls and shutdowns in times of political instability.

Small Media will continue to monitor the implications of the network’s staggered rollout over the course of 2017, and document any incidences of freedom of expression violations in this time.
JANUARY
SHOMA headed into January with a strong hold over the ICT budget for the next fiscal year, and assurances from ICT Minister Vaezi that development work would go ahead as part of the Sixth Five-Year Plan (2016-2021).\(^{117}\) Despite these assurances, there was still critique from Members of Parliament (MPs) regarding the continued delays over the implementation of the project. In addition to that, MPs were concerned about the failure of the ICT Ministry and Supreme Council of Cyberspace (SCC) to keep Parliament updated on the progress of the national network.\(^{118}\)

Perhaps most significantly for this month, Iran signed a partnership agreement with China for cooperation in the ICT sector. This stems from previous announcements by Iran that China will help Iran to launch SHOMA.\(^{119}\) The involvement of China, another state known for its intrusive practices of censorship and surveillance on internet users, certainly provides cause for concern regarding Iran’s moves towards a closed network.

FEBRUARY
Whilst there was little news regarding SHOMA in February, there were continued criticisms over its delayed implementation by conservatives and other hardliners. Thus, we saw public announcements asking those in the ICT Ministry to push for the launch of the national network by September 2016.\(^{120}\) The ICT Ministry also conceded that it had only so far completed 15% of the project.\(^{121}\)

MARCH
March came with yet more promises from ICT Minister Vaezi, who announced that SHOMA, alongside e-Government services, would launch in the next Iranian year (March 2016 to March 2017), which would come with an increase in internet speeds for users. In addition to this, Vaezi stated that the third phase of the ‘Intelligent Filtering’ system would be launched in the near future. At this point, it appeared as though Iran was rolling its censorship system back to the model of the early 2000s, where each ISP was responsible for blocking specific services and content.\(^{122}\)

Mehr News Agency also used the Persian New Year to take a look back at the activities of the ICT Ministry from the previous year (March 2015 to March 2016). In terms of SHOMA, they pointed out that Minister Vaezi had failed to launch the national network, illustrative of the


continued criticism of the Ministry for failing to carry out its promises.\textsuperscript{123}

**APRIL**

April kicked off with Vaezi reaffirming that SHOMA would be launched later in the year.\textsuperscript{124} However, on the same day, the Minister also claimed that it would be difficult for the ICT Ministry to achieve everything that it had promised for the next Iranian year (March 2016 to March 2017). He blamed the fact that Iran’s budget was based on outdated oil prices.\textsuperscript{125}

Despite distancing themselves from their promises, Deputy ICT Minister Nasrollah Jahangard continued to state that SHOMA was a top priority for the coming year.\textsuperscript{126} Vaezi reaffirmed that SHOMA would be launched by September\textsuperscript{127} and that as part of the development of the ‘Resistance Economy’, Vice President Eshaq Jahangiri stated that as part of the ICT Ministry's responsibilities, there would be an increase in the level of user access to the national network, with 20Mbps connections and the development of data centers and content distribution networks.\textsuperscript{128}

**MAY**

May saw more criticisms directed at SHOMA’s implementation, with MP Nasrollah Pejmanfar accusing the Rouhani government of purposefully failing to launch the network, owing to their ‘political objectives’.\textsuperscript{129} In response to such criticisms, on May 15 SCC Secretary Seyed Abolhasan Firouzabadi claimed that it was not constructive to attack delays. Further, he claimed that the success of the project required the cooperation of all three branches of the government.\textsuperscript{130}

Interestingly, Vaezi announced that 85% of SHOMA had been completed.\textsuperscript{131} If true, this would have proved a significant jump from the 15% that his deputy claimed had been completed in February.

**JUNE**

The most interesting critique of SHOMA in June came from Mohammad Jafar Montazeri, the Attorney General of Iran. He claimed that delays to the National Information Network had allowed cyberspace to inflict substantial damage on society. Increased divorce rates and

\begin{itemize}
\item \textsuperscript{131} ICTPress, (2016), ‘Vaezi: I am also a concerned father / ICT Ministry to identify immoral Telegram bots’, retrieved 07/02/2017, http://www.ictpress.ir/news/?item=27922
\end{itemize}
social crimes could, according to Montazeri, be attributed to the poor influence of the internet. On top of that, he asserted that Iran’s enemies had developed careful plans to attack Iranian society through cyberspace.\footnote{ITMEN, (2016), ‘Cyberspace Crisis Headquarters should be established’, retrieved 07/02/2017, http://www.itmen.ir/index.aspx?id=99&articleId=183905}

In terms of the physical development of the project, SCC Secretary Seyed Abolhasan Firouzabadi announced that the price of internet subscriptions for users of Iran’s National Information Network (SHOMA) would drop to a quarter of its current price.\footnote{ISNA, (2016), ‘Price of domestic internet content quartered’, retrieved 07/02/2017, http://bit.ly/2kpPUYI}

In another statement he said that the launch of SHOMA would see the speed and quality of internet access improve dramatically. He added that users would face no additional changes or limitations when using SHOMA, stating that it would offer users the same experience as the global internet, but at higher quality and lower cost.\footnote{ICTPress, (2016), ‘Loans begin to software developers to produce secure multimedia content’, retrieved 07/02/2017, http://www.ictpress.ir/news/?item=28933}

It is interesting that officials place so much emphasis on the quality and cost of the project, whilst specifically denying that the network would impose any restrictions on users. However, given the Iranian government’s track record on internet censorship and surveillance, it is highly likely that the network will be used to bring about greater control.

**JULY**


The month also saw more attempts to draw people into using SHOMA, by inviting mobile app developers to apply for funding and support from the ICT Ministry, so long as their apps are secure and functional on the SHOMA network.\footnote{Mohammadi, Mahdieh, (2016) ‘Under pressure for not filtering Telegram’, Mehr News, retrieved 08/02/2017, http://bit.ly/2krbs9p}

On July 19, a key phase of SHOMA was completed, with the launch of Iran’s data traffic exchange centers.\footnote{Ibid, retrieved 07/02/2017, http://bit.ly/2krbs9p}

**AUGUST**


There also proved some confusion over how the rest of the project would be launched. On August 9, Firouzabadi claimed that it would take place in two phases - the first being the reformation of the existing infrastructure network, and the second involving the launch of the new system.\footnote{Ibid, retrieved 07/02/2017, http://bit.ly/2krbs9p}

However, August 27 saw claims that the platform would be launched in
three phases. Contradiction is, of course, not
something that is new to the Iranian system of
government.

Telegram drew the gaze of officials once more
with Abdolsamad Khorraramabadi, Secretary
of the Commission to Determine Instances
of Criminal Content (CDICC), asserting that
SHOMA necessitates the development
of domestic social media and messaging
applications. Leading from this, he assured the
press that Iranians would one day ‘say goodbye’
to Telegram.\(^{139}\) Grand Ayatollah Naser Makarem
Shirazi also took aim at Telegram, stating that
the network bandwidth allocated for the use of
Telegram should be taken back onto SHOMA,
alongside the development of domestic apps.

Significantly, Shirazi also warned that Iran’s
enemies could use the internet to attack Iran,
pointing to the 2009 post-election unrest
as evidence of foreign interference. He also
criticised the weakness of Iran’s filtering
system, noting how specialists had managed
to bypass the filters in place.\(^{140}\) This critique of
filtering, combined with allusions to the 2009
post-election unrest, in which Iran shut down
the internet, does not bode well for the way
the government plans on using the SHOMA
platform.

August 28 saw the launch of the first phase
of SHOMA in the presence of Vice President

Eshagh Jahangiri, Firouzabadi and Vaezi.
Alongside the launch came the usual claims
that SHOMA aimed to develop a secure
network infrastructure, network independence
and an increase in the use of domestic traffic
amongst Iranian users.\(^ {141}\) In addition to this,
speaking at the launch event Jahangiri stated
a number of statistics regarding SHOMA. The
project cost 200 trillion IRR (6.3 billion USD)
over a period of three years, with 80% of
investment coming from the private sector.
He also asserted that whilst three years ago
90% of Iran’s network traffic was international,
this had fallen to 60%, with hopes that the
second phase of the SHOMA launch would
see domestic traffic increasing to 55%.\(^ {142}\)
Significantly, the Vice President also stated that
all Iranian users must possess proof of identity
in order to use any network. This poses a large
risk to user privacy, giving the government a
quick and easy means to identify users who try
to access content deemed unacceptable to the
government.\(^{143}\)

Despite this, Minister Vaezi claimed that
users should not be concerned about their
information being stored on SHOMA, promising
that individual privacy is the government’s
first priority. He also denied claims that the
network would disconnect Iranians from the
rest of the world. Interestingly, and perhaps
a contradiction to what he had just stated,
Vaezi then claimed that based on Iranian law,


any data requested by the judiciary would be passed onto them. Considering Iran's draconian 2009 Computer Crimes Law, it is highly likely that SHOMA will be used, to some extent, to restrict internet freedom in the country.

### SEPTEMBER
Coming off the back of Vaezi's August comments, Deputy ICT Minister Nasrollah Jahangard insisted that SHOMA is connected to the global internet, and will not cut off Iranians from the rest of the world. Significantly, he went on to mention that the Ministry would be launching a platform that divides domestic and international traffic from each other by the end of September. This proved another concerning development for SHOMA and another contradictory statement from the ICT Ministry, in that the separating of traffic would allow the government to more easily filter content that the Iranian user has access to.

September also saw the continued theme of SHOMA criticism. On September 3, the Supreme Council of Cyberspace (SCC) stated that they were not satisfied with the ICT Ministry's progress on the development of SHOMA, and voted against launching the network. In addition to this, a member of the SCC emphasised that a number of SCC members believed that all the Ministry had done was simply create a data exchange center, rather than the vast National Internet Network that was promised.

### OCTOBER
Despite September's criticisms, Secretary of the SCC Seyed Abolhassan Firouzabadi noted on October 1 that the deployment of the first phase of SHOMA had demonstrated that the ICT Ministry had been following the SCC's guidance on the network's implementation. On the same day, ICT Minister Mahmoud Vaezi announced that the second phase of the National Internet Network would be launched by February 10 2017.

As if to counter criticism and attempt to drum up support for SHOMA, on October 2 Vaezi stated that Supreme Leader Seyyed Ali Khamenei had been following the progress of SHOMA closely for the last thirteen years that it has been in development.

On October 22, the SCC reviewed and approved an agreement relating to SHOMA. The agreement established that the network should be developed based on the principles

---


of social justice and Iran's national needs. Considering Iran's track record on applying principles of social justice to internet freedom in the country, it is confusing as to what the Council is actually referring to.

NOVEMBER
November proved a quiet month for news on SHOMA's development, other than that the ICT Ministry had achieved a number of 'Resistance Economy' objectives related to improving network speeds for SHOMA's users. Deputy ICT Minister Barat Ghanbari noted that average network speeds would increase to 4Mbps by March 2017, with speeds of 20Mbps targeted by March 2021.

DECEMBER
SHOMA had an eventful year's end. ICT Minister Vaezi once more heralded the fast speed, high quality and cheap tariffs that would come from adopting the network, claiming that there would not be any speed limitations on it. On December 10 the Information Technology Organisation (ITO) announced that a new project for SHOMA had been launched. Users of the network would be able to pay their 'departure tax' via the internet.

Although it was still in its pilot phase, they hoped it would be available to users in the near future. December proved a better month for ICT Ministry's relationship with the Supreme Council of Cyberspace (SCC), with the council announcing that it had approved regulations for the National Internet Network. Typically, the SCC also asserted that it had discussed the potential social and cultural impacts of using cyberspace.

As if to prepare for any future setbacks, on December 20 Deputy Minister of ICT Nasrollah Jahangard compared SHOMA to a new-born baby, claiming it will need time to grow and develop. He also noted that the second phase of the network would be launched in February 2017, for the Islamic Revolution Victory Day, and then the third and final phase on May 17 2017, for Telecommunication Day.

At the end of the month, Jahangard asserted that of everything that has been completed so far, 70% of the network has been completed under the control of the private sector. Perhaps most significantly, and to finish off the year for the National Internet Network, on December 28 the Telecommunications Regulatory Commission ordered all mobile networks and Internet Service Providers (ISPs) to distinguish between domestic and

international traffic, supposedly in an effort to decrease tariffs for Iranian internet users. However, the splitting of international and domestic traffic would make it far easier for the government to carry out further crackdowns on internet freedom in the country. Thus, 2016 finished with greater moves towards censorship, surveillance and blocking - a worrying situation to end the year in.

The Big Picture // Domestic Services

With officials consistently blaming a whole host of social and economic challenges on Western-based apps and services, ranging from Twitter, to Facebook, to Telegram, 2016 saw an ever-growing focus on the development of domestic online services. Iran’s Supreme Leader Seyed Ali Khamenei named 2016 the year of "Resistance Economy and Action". An integral part of this ‘Economy of Resistance’, the development of domestic services seeks to draw Iranian users away from Western providers, and instead turn to Iranian-based products – themselves more vulnerable to information controls such as backdoors, interception, and service shutdowns.

Painted as a means to generate more money for the government, and provide more convenience to users, the broader issue with domestic services is the increased control they hand to the government. Domestic services, such as Aparat – an Iranian analogue of YouTube – and CafeBazaar – an Iranian version of the Google Play store – utilise SHOMA’s infrastructure. This, in turn, allows them to provide their users with fast access, providing further incentive for people using international sites to migrate over to domestic platforms. The problem with this is that the closed network of SHOMA gives the government all the tools necessary to filter, monitor, and control the flow of domestically hosted content. Read on as we unveil the development of domestic services over the course of 2016.
DOMESTIC SOCIAL MEDIA
As detailed above, Telegram proved a contentious issue across government last year. And the debate between blocking or filtering Telegram and other non-domestic apps also fed heavily into the development of domestic messaging apps. Perhaps as a response to the obvious flaws in both attempting to filter messaging applications and/or block them, the ICT Ministry sought to invest in and promote the use of domestic applications, as a means to draw people away from their international alternatives. In March, Vaezi said just that - that filtering was “far-fetched”, and empowering domestic platforms was in fact the way forward.158 The Ministry’s May announcement that financial assistance would be provided to companies developing domestic messaging applications thus comes as no surprise. These efforts were further bolstered in June, with the SCC announcing that more would be done to support the implementation of domestic messaging applications.159

September brought more rhetoric against non-domestic social media platforms, with Deputy Minister of ICT Nasrollah Jahangard claiming that the use of foreign social media has an impact beyond security and politics, in that it results in economic loss for the country.160 The former Minister of Defence, Ahmad Vahidi, also observed that social media should be controlled, and infrastructure should be developed to allow for the building of domestic platforms.161

Overall, there was a strong focus on the development of domestic social media networks in 2016, with ICT Minister Vaezi finishing the year stating that the development of these platforms is a top priority for the Rouhani government.162 Although a number of officials claimed that domestic alternatives would bring economic benefits, there is always the overlaying concern that domestic products result in more efficient censorship for the government. Faced with the uncertainty of Telegram’s cooperation, and the difficulty in filtering Telegram’s content, drawing users to domestic versions may appear an easier feat for the government to achieve.

DOMESTIC SEARCH ENGINES
In February, the development of domestic search engines was unveiled as a top priority of the ICT Ministry for the year. Indeed, the government was very generous to those developing domestic services, signified by the signing of a contract worth 1.5 trillion IRR (49 million USD) in order to support domestic companies developing search engines in the same month. By July, the Strategic Council of National Search Engines had signed agreements with 22 companies for 15 projects related to national search engines. Some of these projects were to include: a photograph search engine, a news search engine, map

search engine and a domestic email service, with the total cost amounting to 300 billion IRR (9 million USD).\textsuperscript{163} In the same month, on July 3, Mohammad Khansari, Head of Research, Communications and Information Technology claimed that the domestic search engines Yooz and Parsijoo have 500,000 visitors per year, and cover 2 billion Persian-language pages. This, he claimed, constituted 2\% of Google’s market share, with hopes that the number would increase to 30\% by 2021.

By August 13, the Strategic Council of National Search Engines had finalised agreements for the creation of three local search engines.\textsuperscript{164} On October 1, Alireza Yari, Secretary of the Strategic Council for the National Search Engines Project, said that Iranian search engines offer users a high quality service. Interestingly, Yari also suggested that Iran should implement policies requiring government employees to use national search engines for official business.\textsuperscript{165} Two days later, Amir Ali Kheirandish, Head of the National Search Engines Project, hypothesised that if Iranian users supported domestic search engines, national income from e-commerce would match income from gas exports within a year.\textsuperscript{166} It is interesting to see that throughout the year there is a consistently strong emphasis by officials on the economic benefit of using domestic services.

Despite emphasis on the development of domestic search engines throughout 2016, by November 23, Alireza Yari had conceded that Iranian users were using the search engine Google more than any Iranian alternatives, stating that Iranians make around 100 million Google search requests each day.\textsuperscript{167}

**E-GOVERNMENT SERVICES**

By April 9, Deputy ICT Minister Nasrollah Jahangard had stated that the development of e-Government services were a top priority for the Information Technology Organisation (ITO) in 2016.\textsuperscript{168} This was followed in May with the launch of Iran’s national domestic e-government gateway, which involved the roll-out of 200 services, provided by 60 different governmental organisations.\textsuperscript{169}

e-Government saw further development by June, with the creation of an app named ‘Favakadeh’. The app allows Iranian users to: track their mail deliveries, driver’s licenses, and postage fees, as well as allowing them


to pay their utility bills in-app.\textsuperscript{170} With the increasing speed of IT development, including e-government services, in September the Director of Iran's Passive Defence Organisation (IPDO) pushed for the development of domestic security products in order to maintain sufficient cybersecurity standards. Further emphasis was put on the speedy development of e-government systems in October, when ICT Minister Vaezi announced both that these services would be finalised by February 2017 and that 5,000 more villages would be connected to the internet by November 2016.\textsuperscript{171}

At year's end, there were two significant announcements regarding e-government services. These were the news of a mobile version of e-government being launched in February 2017,\textsuperscript{172} and the unveiling of an e-voting machine at the Iranian International Exhibition of Electronic, Computer & E-Commerce 2016 (ELECOMP).\textsuperscript{173} Interestingly, they claimed that the system had been copied from Brazil. If approved by the Guardian Council, there would be plans to have 50,000 polling stations in Iran.

Overall, 2016 saw significant investment and interest in the development of an efficient e-government service within Iran. Further developments are planned, with the hope that soon all government bodies will be connected to a fully integrated central database, which itself might facilitate the development of new online services for Iranian citizens.


Content Blocking & Filtering in 2016

Iran continued to implement information control methods across 2016, with numerous examples of the Iranian state clamping down on user access. In addition to the usual debates around Telegram, a series of political websites (both reformist and conservative), Western applications, news websites, anti-corruption initiatives, and pornographic (and otherwise ‘immoral’ content) all fell victim to filtering efforts throughout the year.

Filtering in Iran continues to operate on a relatively ad hoc and unpredictable basis, and incidences of website filtering often take place without official statements or confirmation from the ICT Ministry or Filtering Committee. Read on for a detailed examination of the blocking and filtering that took place last year.

For more details about online censorship (along with a full index of the censorship incidents listed below), please visit smallmedia.org.uk/work/filterwatch.
JANUARY
January 2: According to the Mehr News Agency, Telegram users faced disruption in the early morning of January 2. The ICT Ministry responded to the report stating that they have not decided to block Telegram, insisting that the problem did not originate from within Iran.
January 10: According to Mashregh News, Netflix was blocked for several days after launching a service for Iranians. Netflix has been available for Iranian users since January 7.

FEBRUARY
February 3: An anonymous source at the ICT Ministry said a broker has been arrested in connection with an embezzlement investigation. The ICT Ministry has not mentioned his full name and exact role in the ICT industry.
February 8: According to Fars News Agency, the website of the 2016 Beach Volleyball World Tour, held on Iran's Kish Island, has been blocked. Journalists inside the country who want to cover the competition must register for a press pass through the FIVB website, but are currently having a hard time doing so.
February 10: A website belonging to Mohsen Ranani, an economist and lecturer at the University of Isfahan has been filtered. Ranani is reformist who has strongly criticised Ahmadinejad's economic policies. The alternative address of the website is renani.net.
February 28: Ali Jannati, Minister of Culture and Islamic Guidance (MCIG) said his ministry opposes the blocking of Whatsapp and Telegram.

MARCH
March 2: According to Kaleme, the reformist website List-e Omid (The Hope List) was blocked. List-e Omid is a platform used to share the names of nominated reformist and moderate candidates in the parliamentary and Assembly of Experts elections. Pro-reformist and moderate activists launched this website due to a perceived lack of access to media outlets and news agencies for their preferred candidates. Previously, the Expediency Council Secretary Mohsen Rezaee said ‘Iran’s enemies’ achieved electoral successes in large cities because they had access to the Internet.
March 12: Iran’s hardliners launched Mofsedin (The Corrupt), a website to identify users who violate the law on Instagram. According to Mofsedin, they have collected the names of 5,000 accounts, shared their details on their website, and passed them onto the police and intelligence services. In recent years, Iran’s Cyber Army has targeted the accounts of journalists, models, and photographers. (Source)
March 14: A website belonging to the finance and credit institution Samen al-Hoja was blocked by Iran’s Central Bank due to financial issues. (Source)

APRIL
April 3: According to Press TV, Telegram blocked 50 Iranian pornographic channels over a 48 hour period. (Source)
April 11: According to Parsine and user reports, Euronews’ Persian service has been blocked in Iran. Until recently users could access the website without the use of circumvention tools. (Source)
April 18: Kaj Online, a reformist news website in Kermanshah has been filtered. (Source)
April 20: A news website belonging to reformers in Kuhdasht, Lorestan province, has
April 23: An online payment website called Dargah Pardakht has been blocked in Iran. According to users they cannot access to the website any more. The website was similar to Western Union but only for Iran. (Source)

MAY
May 4: Abadeh’s police chief Esmaiel Zeratian announced that the police arrested nine users responsible for creating a WhatsApp group called 18+, and sharing pornographic content to other users. He noted that their group used to send pornographic content on a daily basis, and that it had 200 members in total. (Source)
May 11: According to IT Salam, the Iranian PayPal analogue ZarinPal has been blocked in Iran, and is not longer available for users. (Source)
May 17: According to various website, Aftab News has been blocked and is no longer available for users inside Iran. (Source)

JUNE
June 20: Some Telegram users in the cities of Zabol and Zahedan reported issues using the messaging app. (Source)
June 28: According to Sputniknews, a website belonging to Iranian Ayatollah Dr Seyed Mohammad Hosseini Beheshti has been filtered without any notice or explanation. The website in question was lacking in political content, and it is unclear why the site has been filtered. (Source)

JULY
July 16: It was announced that new ICT Ministry rules require ISPs to separate international internet traffic from domestic traffic for ‘billing purposes’. Although users were informed that they would pay less for domestic traffic as a result, the separation of traffic will empower the Iranian government to discriminate against global internet content (and potentially facilitate shutdowns of international traffic in times of political unrest). (Source)

AUGUST
August 10: Hossein Ramezani, Deputy for Legal and International Relations of Iran’s Cyber Police (FATA) said that three individuals have been arrested for sharing content deemed derogatory and offensive against religious sanctities and the Imams on Telegram. (Source)
August 31: Memari News – an architectural news website – has been filtered on the order of a state prosecutor. Previously Memari News published an article exposing corruption in the municipality of Tehran. (Source)

SEPTEMBER
September 4: Borna News Agency Director Mohammad Mobin, said that his website was filtered by an order of the Commission to Determine the Instances of Criminal Content (CDICC). (Source)
September 4: Amir Mortazavi, News Editor of Moj News said that the website was filtered by an order of the CDICC. He added that both the .ir and .com domains of the website were filtered. (Source)
September 5: According to Shoma News, the news website Nasim Online was filtered. Nasim Online previously shared news about corruption among Iranian officials. (Source)
September 10: Iran’s Court for Culture and Media (ICCM) ordered authorities to stop filtering the Borna News Agency’s website. The site is no longer filtered. (Source)
September 17: By an order of the CDICC,
9Sobh has been filtered. The website belongs to the Executives of Construction Party of Iran. (Source)

OCTOBER

October 5: The Secretary of the Commission to Determine Instances of Criminal Conduct (CDICC) Abdolsamad Khoramabadi denied reports that the filtering of Twitter would be suspended, or that Telegram will be blocked to force Iranians to use domestic apps. He stated that Twitter’s ‘role’ in the 2009 post-election unrest precluded an alteration in filtering policy. (Source)

October 7: Seyed Kamal Hadianfar, Head of Iran’s Cyber Police (FATA) announced that 700 online dating websites have been blocked. He added that only dating websites licensed by the Ministry of Youth Affairs and Sports would be permitted to operate. (Source)

October 26: Mohammad Khani, Head of FATA (Gilan branch) announced that the director of a website was arrested for providing instructions about hacking mobile messenger apps. (Source)

NOVEMBER

November 21: According to a number of online reports the news website Afkar News was filtered. The cause of this is unknown. (Source)

November 28: Hassan Karimi Ghodousi, Director of the National Foundation of Computer Games announced on his Telegram channel that the mobile game Clash of Clans is not filtered, but is suffering from network problems. In the preceding days, users reported difficulties accessing the game, and reported that it had been filtered. (Source)

DECEMBER

December 3: The ICT Ministry announced that problems with Iran’s internet network caused disruption to some Iranians using the Telegraph mobile messaging app and the Clash of Clans game. (Source)

December 5: Nishapur’s Head of Police Akbar Agha Beigi announced the arrest of an ‘immoral group’ that was active on social media. According to Agha Beigi, two males and one female were arrested. (Source)

December 14: Javad Jahanshiri, the Head of the Iranian Cyber Police (FATA) in Khorasan Razavi province, announced that FATA had arrested a member of a poker website as part of efforts to crack down on the illegal practice of gambling. (Source)

December 21: The ‘Jahan News’ website, which was previously filtered due to allegedly sharing false news against the government, was unblocked. (Source)

December 27: The Securities and Exchange Organisation has supported the filtering of 23 unofficial financial and investment advice websites in Iran. The websites had been the subject of fraud allegations and had received a number of complaints from users. (Source)
Summary // 2016 in Review

To conclude, we can describe 2016 as a year of ongoing deadlock between the censorship skepticism of the Rouhani administration, and the authoritarian instincts of conservatives and hardliners with more authoritarian tendencies in the CDICC. Both bodies remain paralysed by the other’s loosely-defined authority – the Rouhani administration is ultimately powerless to overrule the CDICC’s binding decisions on Twitter, Facebook, and other major Western services blocked during the Ahmadinejad period, whereas the CDICC is unable to implement any fresh filtering decisions while the Rouhani administration holds the levers of power in the ICT sector.

Nonetheless, 2016 did not just see a continuation of the status quo – although SHOMA continues to be in development, its initial rollout in September 2016 will likely mark the starting point for the implementation of a new system that could threaten to throttle Iranians’ access to the global internet and help to facilitate future internet shutdowns in times of political unrest. The Rouhani administration has also been very supportive of efforts to develop new domestic services to rival WhatsApp and Telegram, and push these apps out of the Iranian market (although Iran’s characterisation of a cosy relationship with Telegram raises questions here about the urgency they attribute to this effort). The drive to coax Iranian users away onto high-speed, but more easily surveilled platforms is a troubling development that we shall continue to monitor in the coming months.
Altogether though, we would argue that 2016 was a year that clearly reflected the course of ICT policy under Rouhani – at some times seemingly paralysed in the face of challenging institutional tensions, and torn between the promise of a high-tech economic boom and the political dangers of an open and free internet. Rouhani’s government has attempted to steer a middle course, prioritising infrastructure development while deploying moderate (and often rather ineffectual) information controls to attempt to appease more conservative members of the Iranian establishment. Assuming that Rouhani triumphs in the 2017 presidential elections, Small Media predicts that such contradictions will continue to define his presidency in the months and years to come.
References

- Akbarpour, Nima, [@nima], 'If Telegram servers move inside Iran...', Twitter, 16/08/2016, retrieved 07/02/2017, https://twitter.com/nima/status/765478626733228032
- Click.ir, 'Aparat Application was Removed from Cafe Bazaar', http://click.ir/1395/07/26/aparat-applications-was-removed-from-cafe-bazar/
- Apple Communities, retrieved 07/02/2017, https://discussions.apple.com/thread/5115805?start=0&tstart=0
- Bakhshipour, M., 'Our policy is to


روحانی و احمدی نژاد در آمار


reuters.com/article/us-dutch-iran-hacking-idUSTRE7831HS201110906.


*Where does my money go?*, Website, retrieved 8/8/2016: [http://app.wheredoesmymoneygo.org//about.html](http://app.wheredoesmymoneygo.org/about.html).

