2. INTERNET CENSORSHIP IN IRAN: PREVENTATIVE, INTERCEPTIVE, AND REACTIVE

by Kyle Bowen and James Marchant

The Iranian authorities adopt a triangulated approach to internet censorship and surveillance. Preventative, interceptive, and reactive measures are intertwined and form a coherent overall strategy for internet control.

When Tim Berners-Lee invented the World Wide Web, he built a model that was open, decentralised and accessible to all. Today, that vision is being subverted in the face of a dramatic expansion of state interference in the digital realm. Increasingly, governments are using the internet to spy on their citizens, and in few places is this more apparent than Iran.[1]

Iran's pervasive programme of online censorship has seen it labelled as one of the 'twelve enemies of the Internet' by Reporters Without Borders (2012a), and described as the 'least free' country in terms of internet freedom by Freedom House (Kelly and Cook, 2011).

The Iranian government frequently cracks down on platforms and content it considers to counter the values of the state. In other media, this is a fairly straight forward task: authors must seek permission from the Ministry of Culture and Islamic Guidance before publishing their books, musicians require authorisation before releasing their work, and domestically-produced television is controlled entirely by the national broadcaster, IRIB. The internet, however, provides Iranian users a link to the outside world that is far more difficult to control.

This chapter seeks to answer a number of key questions about the past, present and future of internet censorship in the Islamic Republic, identifying the state authorities' rationale for imposing censorship, the tools used to enforce it, and the individuals and government bodies that are responsible for overseeing it.

[1] All countries monitor and/or censor the internet, but the Iranian case is quite exceptional in its scope and intent. The political establishment has identified a number of cultural and political threats inherent in the structure of the internet and has moved to regulate it accordingly.

A Tangled Web: The Chaos of Internet Policy Making in Iran

A complex network of bodies determines state internet censorship policy in Iran, each holding a set of rather poorly-defined powers and responsibilities, resulting in numerous disputes between different sets of policy makers and enforcers. To compound this confusion, a number of influential policy-makers sit on several committees simultaneously, each with overlapping agendas, responsibilities, and approaches to internet policy.

This institutional chaos has manifested itself in several examples of confused government policy, resulting in some very high-profile power struggles between key political actors. The conflicting messages emanating from the government regarding social media illustrate this. For instance, while Facebook and Twitter are officially blocked in Iran, with users forced to deploy illegal circumvention tools to access them, many senior officials openly flout these rules for their own self-promotion.[2]

Statements from high-profile officials are also contributing to the confusion around social media policy. In a statement in March 2014 Ali Jannati, the Rouhani-appointed Minister of Culture and Islamic Guidance spoke of the need to unblock Facebook, conceding that at least 4 million Iranians already make use of the platform, and arguing that the government is fighting a losing battle by attempting to maintain the ban (Fararu, 2014). President Rouhani struck a similar chord in a televised address in September 2014:

> *Some people think we can fix these problems by building walls, but when you create filters, they create proxies... this [current policy] does not work. Force does not produce results.*
>
> President Hassan Rouhani (The National, 2014)

Hardliners remain staunchly opposed to any relaxation in national filtering policy. In response to Jannati's speech, Abdolsamad Khoramabadi, the Secretary of the 'Commission to Determine the Instances of Criminal Content' (CDICC) - Iran's official censorship body - responded that there are no plans to reverse the policy of filtering sites such as Facebook.

[2] Many high-ranking officials maintain accounts on forbidden social media platforms, including the Iranian president, Mr Hassan Rouhani (twitter.com/Rouhani_ir), Foreign Minister Mohammad Javad Zarif (facebook.com/jzarif) and Supreme Leader Ali Khamenei (instagram.com/khamenei_ir and twitter.com/khamenei_ir)

The War Over WhatsApp

In May 2014, the CDICC passed a motion to ban the mobile messaging application WhatsApp, a decision opposed by Rouhani and Mahmoud Vaezi, his ICT Minister. The subsequent policy confusion and internal political wrangling provide a particularly clear example of the complex and often chaotic processes involved in formulating and executing censorship policy in Iran.

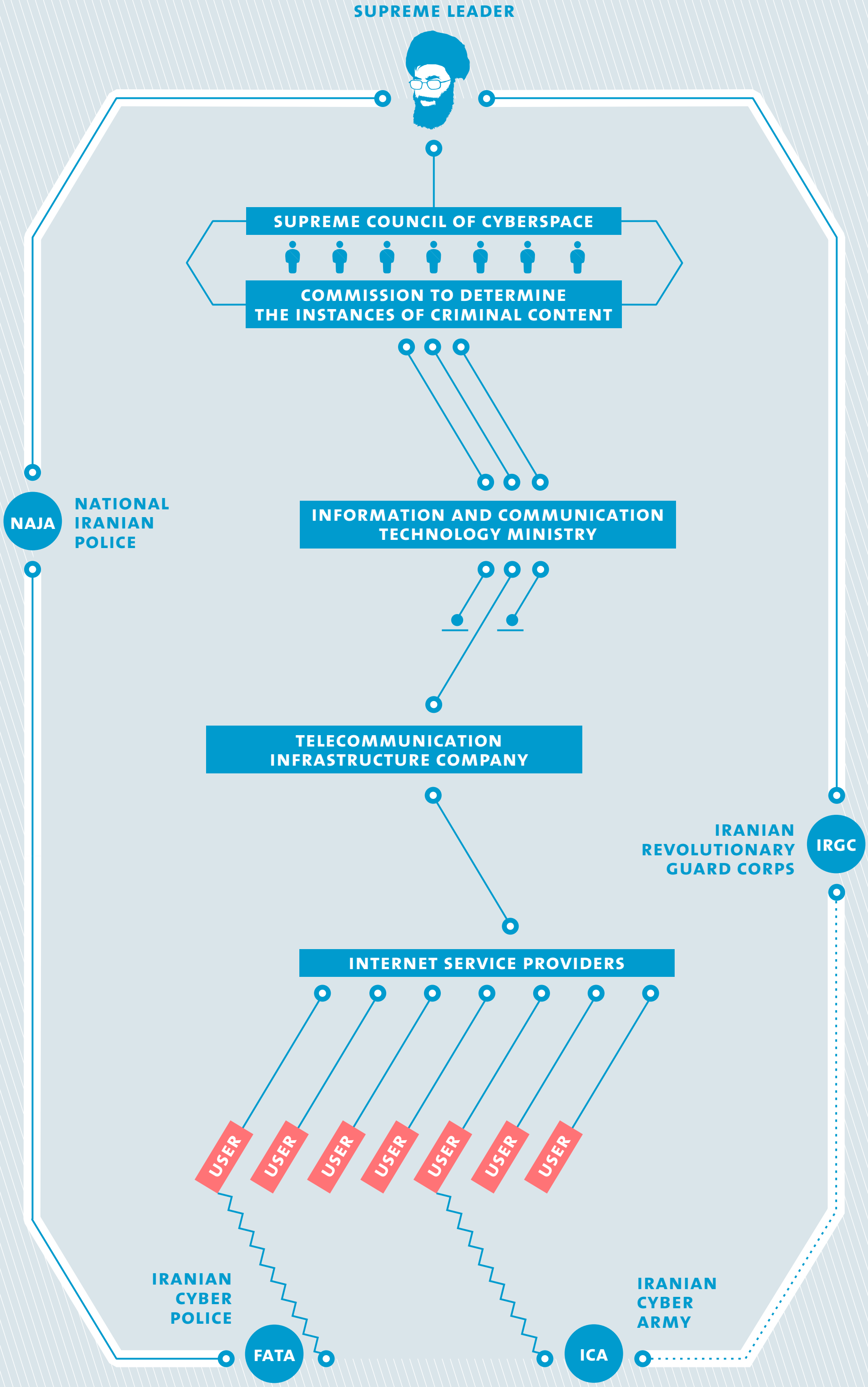
The CDICC initially proposed the ban of WhatsApp on April 30 2014, shortly after Facebook's $19bn acquisition of the messaging app.[3] President Rouhani challenged the CDICC's proposal, ordering the plans to block WhatsApp to be abandoned in a meeting of the Supreme Council of Cyberspace (SCC), which he chairs (Khodabakhshi, 2014). Whilst all the other censorship bodies are nominally subordinate to the SCC, this is the first occasion in which either the President or the Council has chosen to intervene publicly in filtering issues. Consequently, Rouhani's move was extremely controversial, and contributed to widespread confusion over the roles and responsibilities of the SCC and the CDICC.[4]

The authority of the SCC has been asserted most vociferously by members of Rouhani's cabinet, with ICT Minister Mahmood Vaezi arguing that President Rouhani and the SCC are responsible for managing all policy relating to social networks and that CDICC must comply with all SCC rulings (Tasnim News, 2014a). However, the SCC's authority is not universally accepted, and a number of figures have denounced Rouhani for his direct intervention. Hardline CDICC Secretary Abdolsamad Khoramabadi once again emerged as a leading critic of the government, insisting that the President lacks the authority to overrule CDICC orders, and demanding that the government execute his body's rulings (Fars News, 2014a).

In the visualisation overleaf, we plot out the chaotic structure of Iran's online censorship and surveillance system, and the various authorities sturggling to control it.

[3] In addition to having been blocked for its association with Facebook, some have argued that a primary motivation behind the decision to block WhatsApp was to protect domestic mobile service providers from a decrease in revenue by forcing users to continue texting rather than making use of free messaging services.

[4] The roles and responsibilities of Iran's internet policy-making bodies are not clearly demarcated. This ambiguity has ignited inter-factional and inter-committee conflicts and resulted in the formation of muddled and ineffective government policy. As a result, Iranian internet users are never entirely sure of the boundaries and limitations governing their online behaviour.



SUPREME LEADER

SUPREME COUNCIL OF CYBERSPACE

COMMISSION TO DETERMINE THE INSTANCES OF CRIMINAL CONTENT

INFORMATION AND COMMUNICATION TECHNOLOGY MINISTRY

TELECOMMUNICATION INFRASTRUCTURE COMPANY

INTERNET SERVICE PROVIDERS

USER

USER

USER

USER

USER

USER

USER

NAJA

NATIONAL IRANIAN POLICE

IRGC

IRANIAN REVOLUTIONARY GUARD CORPS

IRANIAN CYBER POLICE

FATA

ICA

IRANIAN CYBER ARMY

figure 1: **WHO IS RESPONSIBLE FOR CENSORSHIP?**

Policy Making (Official)

Supreme Leader (SL)
Most powerful decision maker in Iran has legislative and policy-setting powers over internet communications.
Appoints directors of key military, security and governmental posts involved in bodies that censor the internet such as:

- The ommission to Determine the Instances of Criminal Content (CDICC)
- The Iran Cyber Police - FATA

Supreme Council of Cyberspace (SCC)
Established as the result of a directive issued by the Supreme Leader in March 2012.

Top policy-making body for cyber activities in Iran.

Formed by SL to develop the state's domestic and international cyber policies

Commission to Determine the Instances of Criminal Content (CDICC)
Responsible for identifying web content to be filtered and blocked.

More conservative than the SCC creates lists of illegal websites and online content that violates public morals, contradicts Islam, threatens national security, criticises public officials or organisations, or promotes either cyber crimes or the use of circumvention tools.

The SCC and CDICC share seven common members which illustrates the lack of a coherent division of powers and responsibilities between policy makers and those implementing censorship decisions.

Executive (Official)

Information and Communication Technology Ministry (ICT)
Responsible for executing the filtering list from the CDICC.

Responsible for launching the National Information Network (SHOMA)

Manages the Internet network and all communication infrastructures.

Telecommunication Infrastructure Company (TIC)
The only company that has exclusive rights to buy Internet bandwidth for Iran.

Cyber Police (FATA)
A division of Iran's police department established in January 2011 to combat cybercrimes such as scams, fraud, etc.

Executive (Unofficial)

Iranian Cyber Army (ICA)
An underground network of pro-regime cyber activists, hackers and bloggers. Monitors the internet and launches cyber attacks on opposition and anti-Islamic websites.

Operates under the Intelligence Unit of the Revolutionary Guard.

Iranian Revolutionary Guard Corps (IRGC)
The branch of Iran's military established not for the purpose of defending Iran from external threats, but instead with the purpose of upholding the 'Islamic system' of the Republic.

The intelligence wing of the IRGC is widely understood to be involved in supporting and co-ordinating the offensive cyber-warfare activities of Iran's 'Cyber Army', although no official relationship has been publically confirmed.

Neutral

Internet Service Providers (ISPs)
Buys Internet bandwidth from TIC and sells to Iranians.

Plays no role in internet censorship

APRIL 30, 2014

CDICC

We have passed motion ordering the **ICT Ministry** to block **WhatsApp**

MAY 4, 2014

ICT Minister Vaezi

On the request of **President Hassan Rouhani**, the Ministry refuses to block WhatsApp.

MAY 4, 2014

CDICC Secretary Abdolsamad Khoramabadi

The President does not have the power to suspend **CDICC**'s orders, **Rouhani**'s government (including the **ICT Ministry**) must execute the committee's rulings!

MAY 6, 2014

ICT Minister Vaezi

No! The CDICC must comply with all the rulings of the **SCC** and **President Rouhani**.

JUNE 17, 2014

SCC member Alireza Shahmirzae claims that the SCC has not yet made a decision about blocking WhatsApp.

JUNE 18, 2014

A member of CDICC

The committee has no current plans to block mobile chat apps such as WhatsApp.

According to an unnamed CDICC member, the committee voted against blocking WhatsApp in its most recent meeting.

figure 2: WHATSAPP CASE STUDY

April 30
CDICC passes motion ordering the ICT Ministry to block WhatsApp

May 4
ICT Minister Vaezi announced that the Ministry would not block WhatsApp, on the request of President Hassan Rouhani.

May 4
CDICC Secretary Abdolsamad Khoramabadi said that the President does not have the power to suspend CDICC's orders, and insisted that Rouhani's government (including the ICT Ministry) must execute the committee's rulings.

May 6
ICT Minister Vaezi stated that the CDICC must comply with all the rulings of the SCC and President Rouhani.

June 17
SCC member Alireza Shahmirzae said that the SCC has not yet made a decision about the blocking of WhatsApp.

June 18
A member of CDICC stated that the committee has no current plans to block social mobile apps such as WhatsApp. According to the unnamed member, the committee voted against blocking WhatsApp in its most recent meeting.

For Every Occasion: Iran's Censorship Toolkit

The Iranian authorities adopt a triangulated approach to internet censorship and surveillance. Preventative, interceptive, and reactive measures are intertwined and inform a coherent overall strategy for internet control:

- *Preventative measures* are designed to stop Iranian users from accessing forbidden content in the first place, and are not geared towards monitoring and threatening individual uses.

- *Interceptive measures* exist to silently track and thwart individual users who have managed to work around the state's preventative security infrastructure.

- *Reactive measures* are used to gather intelligence on general internet usage patterns, which are then fed back into the development of preventative and interceptive structures. These measures also target individual users whom state authorities have identified as persons of interest.

Nipped in the Bud: Preventative Methods

The primary purpose of preventative methods of internet censorship is to prevent Iranian netizens from accessing content deemed 'immoral' by the religious establishment. Preventative methods do not punish or harm the user; their purpose is simply to make content inaccessible, or to at least complicate access.

DNS redirection and URL blacklisting

Early technology used by the Iranian government to block online content was clumsy, and only capable of filtering entire websites at the domain level.[5]

The responsibility for this DNS redirection process has since been transferred to the Telecommunications Infrastructure Company (TIC), the state-run company responsible for purchasing Iranian bandwidth from international networks and selling it on to Iranian ISPs (Islamic Parliament Research Centre, 2014: 16). The TIC applies its content filters prior to selling bandwidth on to ISPs, meaning that by the time bandwidth reaches ISPs, it has already been 'cleaned'.

[5] Previously, ISPs were given lists of URLs to block, and words to ban from search requests. DNS redirection was then used to forward illegal web requests to a webpage managed by censors.

Content-control software, HTTP host and keyword filtering

The employment of content-control software, along with HTTP host and keyword filtering, remains the most widely used method of filtering at the present time. With HTTP host and keyword filtering, authorities block access to certain sites by manipulating connections based on their HTTP host headers, and to URLs containing certain keywords.[2] This task is performed by content-control software installed by the TIC, which automatically inspects and filters web content, as well as monitoring IP traffic and internet-user activities.

In 2013, the Small Media design team conducted research on the 100 most-viewed pages in Persian on Wikipedia. Wikipedia isn't blocked in Iran, but specific pages within it are. To test the links for filtering we set up a VPN connection to a computer based inside Iran. Wikipedia, a website with a 'radically open' approach, poses a stark contrast to Iran's closed society.

Small Media produced an infographic from the data called '*Closed Society Meets Open Information*'. Our analysis demonstrated the types of information the government seeks to block. The results showed Wikipedia to be predominantly 'open', with only 16 out of the 100 pages blocked. 10 of these were related to sexuality ('sexual intercourse', 'homosexuality', 'vulva', 'masturbation'), with the remaining 6 pages suggesting Iran's nervousness around access to historical and religious information (Small Media, 2013a).[7]

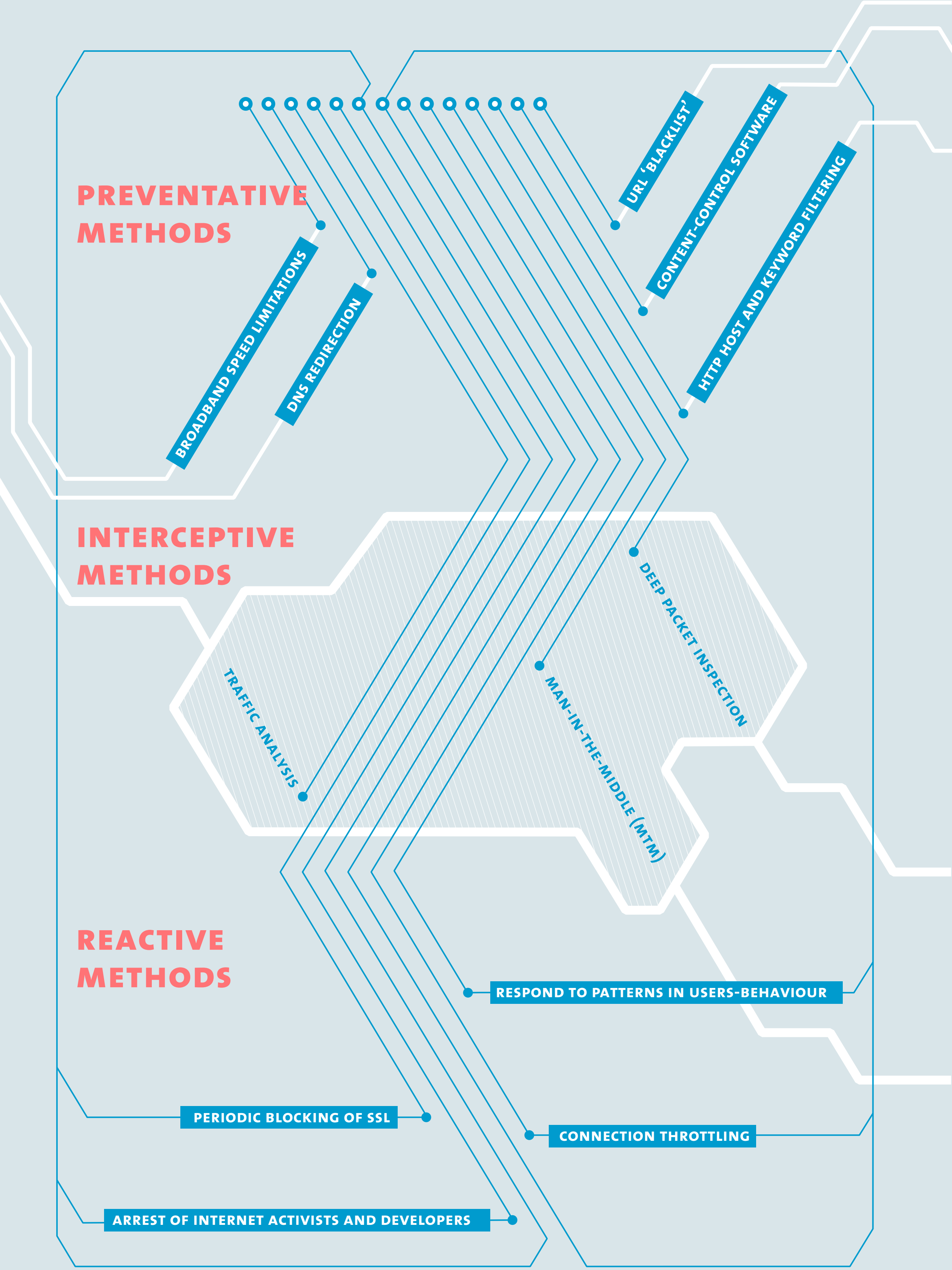
Broadband speed limitations

Preventative censorship is not limited to content filtering; infrastructural shortcomings and legislation also inhibit access. In 2006, the Ministry of Communication and Information and Communications Technology forbade ISPs from providing private users with internet connections faster than 128 KB/s. There are exceptions to this rule, with professionals and students being granted access to more bandwidth.

Compounding the issue of broadband speed limitations is the fact that circumvention tools, which are used by around 70% of young internet users to evade government filtering (ISNA, 2014), dramatically decrease internet speeds. In conjunction with existing speed restrictions, it is incredibly difficult for the average Iranian user to access multimedia content online.

[6] The list of prohibited keywords originally only contained terms frequently used to access adult content, but this list has been expanded in the wake of the unrest that accompanied the 2009 presidential elections.

[7] The other blocked pages were Cyrus the Great, Facebook, Ruhollah Khomeini, Suleiman I, Shahin Najafi, and Akbar Hashemi Rafsanjani.



PREVENTATIVE METHODS

URL 'BLACKLIST'

CONTENT-CONTROL SOFTWARE

HTTP HOST AND KEYWORD FILTERING

BROADBAND SPEED LIMITATIONS

DNS REDIRECTION

INTERCEPTIVE METHODS

DEEP PACKET INSPECTION

TRAFFIC ANALYSIS

MAN-IN-THE-MIDDLE (MTM)

REACTIVE METHODS

RESPOND TO PATTERNS IN USERS-BEHAVIOUR

PERIODIC BLOCKING OF SSL

CONNECTION THROTTLING

ARREST OF INTERNET ACTIVISTS AND DEVELOPERS

figure 3: METHODS OF INTERNET CENSORSHIP

Preventative Methods

Methods used to prevent forbidden content from reaching Iranian users in the first place.

URL 'blacklist'
When a user attempts to access blocked content, they are automatically redirected to a webpage managed by censors

DNS redirection
Telecommunications Infrastructure Company (TIC) is given a list of URLs, which it blocks prior to allocating bandwidth to ISPs

Content-control software
Software used by TIC to automatically inspect, filter, and block sites

HTTP host and keyword filtering
URLs and headers containing specific text are automatically filtered by TIC

Broadband speed limitations
ICT Ministry forbids speeds faster than 128kbps for home users

Interceptive Methods

Methods used to monitor and block forbidden content from reaching users as they access it.

Deep Packet Inspection
Technology used to monitor, track and block internet traffic

MITM (man-in-the-middle)
Method used to intercept online communications

Traffic Analysis
Analysis of sites that are being viewed most frequently

Reactive Methods

Methods of censorship and control used to respond to users after they have gained access to restricted content.

Respond to patterns in user-behaviour
Traffic analysis and DPI surveillance informs the creation of updated blacklists and filtered keywords

Arrest of internet activists and developers
The state has arrested a number of cyber-activists working against online censorship

Periodic blocking of SSL
Websites with SSL security protocols are periodically blocked inside Iran, forcing users to use insecure websites instead.

Connection throttling
At moments of political or social tension, connection speeds are throttled to limit online engagement

These preventative filtering methods aim to strangle off the internet as an alternative space for accessing restricted content and engaging in activity deemed 'subversive' by state authorities. Despite users' best efforts to get around the state's filtering techniques, there is little they can do to avoid the frustrations of Iran's glacial broadband speeds.

Cat and Mouse: Interceptive Methods

The Iranian authorities also use a far more sinister tactic in their censorship regime: data interception. Unlike filtering and other forms of preventative censorship, interceptive methods are active, invisible, and unpredictable.

Deep Packet Inspection (DPI)

The technology that enables this interceptive form of censorship is called Deep Packet Inspection (DPI), and it is used to analyse email content and track browsing history. Analysts have commented that DPI surveillance methods have been in practice since the 2009 post-election unrest (Parsons, 2011).[8]

The journalist and cyber-activist Walid al-Saqaf described the implications of expanded DPI surveillance in a February 2012 interview with Arseh Sevom.

> *The idea behind [DPI] is if you access a certain protocol or a particular service, then the Iranian government actually goes into the header or the inner traffic and analyzes them bit-by-bit to check what is going through, and then compare that to a stack of black list arguments, and if it matches it closes the network. That has caused a tremendous internet slowdown in Iran.*
>
> Arseh Sevom, Breaking and Bending Censorship with Walid al-Saqaf (2012)

Man-in-the-Middle

DPI is also the technology behind 'man-in-the-middle-attacks' (MITM).[9] These MITM attacks are often small in scope but can last for protracted periods. In 2011, an Iranian Google user was informed by a Chrome security alert that the certification for their Gmail account was fraudulent. Upon further investigation, they discovered that the fraudulent certificates had been in place for two months, meaning that attackers may have been privy to the user's private conversations and

[8] In 2012 the International Telecommunications Union (ITU) put forward international standards for the use of DPI technology (ITU, 2012), but these standards do not delineate how specific technologies should or could be used. There has been very little consideration for the implications of standardising the use of this technology.

[9] In MITM attacks, the attacker takes position in the middle of a private interaction between two endpoints. Unbeknownst to both users, all information filters through this MITM.

email exchanges for the entire period (Schoen and Galperin, 2014). The authorities have not claimed responsibility for this MITM attack, but assaults such as these reveal the online risks faced by activists and the bounty of information that the state could gather from unsuspecting users.

Anonymous or Not?

There are a number of tools available to Iranian users to help them evade these pervasive surveillance techniques. Tor, one program commonly used for this purpose, directs internet traffic through a free, worldwide, volunteer network consisting of more than five thousand relays, concealing the user's location and internet usage from anyone conducting network surveillance or traffic analysis. In this manner, Tor enables Iranian users to securely access filtered and restricted segments of the internet.

However, such methods are not without their drawbacks. Using circumvention tools slows browsing speeds down to a crawl. And whilst governments are generally incapable of decoding anonymised traffic online, they can easily distinguish between encrypted and unencrypted traffic, meaning that they can block all encrypted traffic with relative ease.

The Iranian government did so for two months in July/August 2014, preventing 75% of the network's estimated 40,000 daily users from connecting to Tor (Alimardani, 2014). However, online activists quickly devised a solution: they began to employ 'pluggable transports' - Tor connections that connect to the wider network using a hidden pathway known as a 'bridge' - making it far more difficult for authorities to detect and block traffic.[10]

In this way, Iranian users are often able to sidestep the government's efforts to intercept and block their online activities. Yet in spite of this, state authorities continue to work to gather information and intelligence about users' web habits, in an effort to revise and strengthen Iran's online security apparatus.

[10] Tor has gained 3000 new users since it was blocked in July, all of whom are using bridges outside of the regular Tor connections (Ibid, 2014).

Feedback Loop: Reactive Methods

In addition to preventative and interceptive methods of internet censorship, Iran also deploys reactive methods. Instances of reactive censorship typically arise either in response to long-term patterns in user behaviour, or to high-profile cases that unnerve the authorities. Reactive censorship is the most difficult to assess, as it is by nature less consistent than other forms of filtering in that it responds to the strategies and evasive tactics utilised by Iranian users. While the high-profile arrests of internet activists and developers might serve to deter other internet users from breaking the 'rules', technology also plays a large role in reactive censorship.

SSL and the 'Second Wave' of Internet Censorship

Iran's internet censorship methods have increased dramatically in sophistication in recent years, as authorities have been working to counter the efforts of users to gain free and unrestricted access to forbidden content.

Many users have been able to protect themselves from MITM attacks by making use of Secure Sockets Layer (SSL) protocols. The Iranian authorities have periodically blocked SSL websites, offering a clear indication of their intentions. By blocking SSL protocols, netizens are forced to use insecure sites, putting themselves at greater risk of MITM attacks. The International Campaign for Human Rights in Iran argues that the government's efforts to undermine user security marks a profound shift in government censorship policy.

> *SSL blocking can... be seen as the second wave of Internet blocking in Iran. Until now, the Iranian regime has only blocked websites, which in its worst form constituted censorship and a violation of the users' right to free access to information. But in this second wave of blocking, the blocking of security protocols is targeting the very security of Internet users.*
>
> ICHRI, "Iran's New Methods of Internet Filtering Put Users at Risk" (2014)

This 'second wave' of integrated internet censorship and surveillance is also reflected in the 2009 Computer Crimes Law, which requires ISPs to retain records of all data uploaded or downloaded by users for a 3-month period. Coupled with the repeated blocking of SSL protocols, ISPs are able to retain access to vast reams of personal data, all of which is accessible to the government.

[11] SSL protocols are security protocols that transmit encrypted information between users and websites (identified by their URLs, which begin with 'https'), thereby enabling Iranian citizens to share information online in a secure manner.

Cracking Down

The availability of all this information allows the government to exercise impunity in cracking down on dissidents and cyber activists. Access to vast repositories of user data is enabling the government to rapidly identify suspects, and then arm themselves with mountains of evidence for use in interrogations and trials.

Saeed Pourheydar, a journalist arrested in 2010, said that the intelligence officers who questioned him brandished transcripts of his phone conversations, and of email and SMS exchanges. These claims appear to be legitimate. Fellow inmates told Pourheydar that they had similar experiences (Elgin, Silver and Katz, 2011), while the activist Saleh Hamid, a university student in 2010, reported that recorded phone conversations were used against him in interrogations (Secklow, 2012).

Internet Cafes - A Home Away from Home?

Previously, many users attempted to protect their privacy by using internet cafes, thereby preventing the government from tracing their online activity back to their home address. The lack of regulation around internet cafes provoked the government into engaging in frequent crackdowns on cafes that played host to 'illicit' online activities, with 24 cafes raided and shut down in a single day in January 2007 (Reuters, 2007). However, such raids were ineffective as a means of deterring individuals from using internet cafes for unlawful activity, and so in 2012 the government reacted, introducing an additional measure of censorship by imposing stringent new regulations on internet cafes.

Under these new regulations, customers of internet cafes are required to present photographic ID and agree to being filmed by surveillance cameras before being permitted to go online. Internet cafe managers are required to keep these video recordings, full identity records, and the browsing history of their customers for six months after their visit (Esfandiari, 2012).

These government measures have made it more difficult for Iranian citizens to surf the internet safely in public. Authorities have been able to pinpoint the origin of 'illicit' activities down to a specific computer, at a specific time, allowing them to quickly identify users.

Reinforcing the Surveillance State

The reactive forms of monitoring and intelligence-gathering that we have discussed are central to Iranian authorities' efforts to continuously enhance the efficiency and reach of the surveillance state. The information gathered through the development of rigorous regulatory systems for internet cafes and ISPs, and the weakening of user security through the targeting of SSL-enabled servers, directly inform and expand the body of preventative methods used by the authorities to inhibit internet access.

Connection Throttling

Connection throttling is another method of reactive censorship deployed by authorities to restrict access in response to short-term political or social events. During the protests that followed the 2009 presidential elections, connection speeds to webmail services such as Gmail were significantly hindered. This process has been repeated numerous times since, to the point where internet connection speeds have become a measure for the political situation of Iran. On the eve of significant dates that could give rise to demonstrations, the connection speed is slowed down to prevent the circulation of photos and videos.

> *The reduction of the internet speed, which some called 'disturbances', was the result of security measures taken to preserve calm in the country during the election period.*
>
> Former ICT Minister Mohammad Hassan Nami, (Esfandiari, 2013)

The state is very forthright about this. Given this unusual openness, it seems such efforts to choke off users' internet access during periods of political tension will continue to form a central component of the state's 'emergency response procedures' in the future.

Hide and Seek: Circumvention Tools in Iran

As we've discussed already, Iranian users are being forced into constant technological innovation in order to outsmart and outmaneuver the state censors. Although a considerable volume of online content is blocked or filtered by the Iranian authorities, users utilise a variety of sophisticated circumvention tools to bypass these restrictions and access blocked websites.

Ducking and Diving

Circumvention tools are fairly ubiquitous, meaning that blocked websites like Facebook and Twitter remain hugely popular in Iran. A September 19 report by Iran's Ministry of Youth and Sports found that 69.3% of Iranian youth are users of circumvention technologies such as proxies or VPNs (ISNA, 2014), demonstrating the extent to which circumvention tools are posing a challenge to Iran's system of internet filtering. The state has attempted to respond. According to the 2009 Cyber Crime Law, it is illegal to distribute any kind of circumvention tool allowing users to bypass the filtering system, or to instruct people how to use such tools (Kelly, Cook and Truong, 2012).

It remains unclear whether the sale and use of VPNs is legal under Iranian law. The ambiguity arises from the fact that VPNs are not technically circumvention tools; their primary purpose is to assist private companies in securing their online communications networks. However, tech-savvy Iranians have increasingly made use of VPNs to bypass sophisticated government internet filtering, using them to connect to proxy servers.

Divided

This situation has prompted some conflicting statements about VPNs from Iranian authorities. In October 2011, Reza Taghipour, a member of the SCC and the former ICT Minister in Ahmadinejad's government, declared the use of VPNs illegal, prompting the Telecommunication Company of Iran (TCI) to impose restrictions on their sale. Yet the MP (and long-time Ahmadinejad critic) Ali Motahari protested that the use of VPNs is indeed permissible under Iranian law, arguing that neither Taghipour's statement nor the action of the TCI had any legal grounding. Recently, however, there have been signs that authorities are attempting to clarify the legal position of VPNs. In May 2014, Kamal Hadianfar, head of Iran's Cyber Police (FATA) announced that Iran's Parliament is currently reviewing the legal status of VPNs, stating that moves will likely be taken to prohibit their usage and sale pending the passage of new legislation (Khabar Online, 2014a).

Although the sale of VPNs has not been explicitly outlawed, this hasn't stopped FATA from making a number of arrests relating to the sale of the tools.

- *10 April 2013*: A young man who sold VPNs and other circumvention tools was arrested by FATA in Qazvin Province (Mashregh News, 2013).

- *5 July 2013*: A 35-year-old man who used another person's identity to sell VPNs was arrested by FATA in Tehran Province (ISNA, 2013).

- *12 March 2014*: An individual who sold VPNs and provided support to users for more than 3 years was arrested by FATA in Razavi Province (Fars News, 2014b).

- *13 April 2014*: A blogger who sold VPNs and other circumvention tools was arrested by FATA in Kerman Province (Tasnim News, 2014b).

At the same time as it has been working to crack down on VPN sellers, the Iranian government has attempted to enter the VPN market in an bid to curtail the usage of VPN technology to evade censorship. The most high-profile effort was launched in March 2013, when the Supreme Council of Cyberspace (SCC) attempted to outlaw the sale of 'unrecognised' VPNs, instead promoting the sale of an 'official' TIC-developed alternative (Small Media, 2013c).

Just 26 VPN companies applied to register with the state-sanctioned (and state-monitored) TIC VPN, and the trade in unregistered VPNs carried on much as it did before the scheme was introduced. By June, the TIC conceded that the project had failed, and announced its cessation (Small Media, 2013c). Iran appears to be struggling to determine a coherent policy to respond to the challenge posed by the popularity of VPNs and circumvention tools. Though it has attempted punitive crackdowns on sellers, as well as market regulation and co-optation, its efforts have so far failed to dissuade Iranians from using the tools to sidestep the country's filtering system.

So What Does the Future Hold?

With the 2013 election of the moderate President Hassan Rouhani, hopes were raised that Iran would see an easing of the pervasive censorship system and an accompanying opening of the internet. Rouhani had indicated on a number of occasions that this was his intention, publicly stating that he believes in the rights of all Iranians to access information freely, and insisting that his government's efforts are geared towards this end (NBC News, 2013). Rouhani has also commented on the futility of trying to limit the open nature of the internet.

> *We are living in a world in which limiting information is impossible. Youth are faced with a bombardment of information and we must prepare to handle it.*
>
> Hassan Rouhani during the 2013 presidential campaign (CITNA, 2013)

But a year and a half into Rouhani's presidency, we are yet to see the fulfilment of these promises. Access to Western-produced social media networks such as Facebook and Twitter remains restricted, and the availability of a number of mobile communications apps such as WeChat has been curtailed.

Despite high hopes following the 2013 election, the extent of censorship in Iran shows no signs of diminishing. So what does the future hold? The answer to this question largely depends upon the future of two major government projects: 'Intelligent Filtering' and the 'National Information Network' - also known as SHOMA.

Intelligent Filtering

On 24 January 2014, SCC member Mehdi Akhavan Behabadi made a statement in which he argued that the grievances expressed by users about Iran's filtering processes are largely born from the clumsiness of the country's methods. He believes that Iranians are not campaigning for access to 'immoral' content, but instead for a smarter system, and has indicated that a new form of 'intelligent filtering' technology is being developed to enable authorities to block specific items of content on websites, rather than entire domains, as is currently the case (Mehr News, 2014). These plans were later confirmed by the SCC secretary, Mohammad Hassan Entezari.

> *Some universities and private companies have been working to design an intelligent filtering system for the Internet that will be able to block specific parts of websites based on their content. In the near future... the Iranian people will begin to see less intrusive censorship methods being implemented.*
>
> Mohammad Hassan Entezari, SCC Secretary, 29 January 2014 (Khabar Online, 2014b)

The National Information Network - SHOMA

For the past decade the government has spoken intermittently about creating an independent, country-wide network that will host important domestic online services. This network is intended to be fully monitored and censored, hosting only 'clean' content that is 'compatible with religious and revolutionary values.'

SHOMA project is being conducted in four primary phases:

1. The construction of a network capable of separating local and international traffic. SHOMA will be an independent high-speed network that connects all government organisations.

2. The hosting and registration of Iranian websites on local servers and .ir domains respectively.

3. The provision of domestically developed applications and services including an OS, email service, search engine, and communication apps.

4. The production and promotion of online content
(Small Media, 2014a: 7)

There is a growing fear amongst Iranian internet users that SHOMA is being constructed as a replacement for the global internet and that once the network is completed, and state authorities no longer rely on the global internet to provide them with essential services, they will cut off access to the World Wide Web (Seifi and Knight, 2012).

These fears were compounded by statements made by the Ahmadinejad-era Head of Economic Affairs, Ali Agha-Mohammadi. Although he acknowledged that the new network would initially operate parallel to the internet, he went on to speculate that SHOMA could end up replacing the global internet in Iran, as well as in other Muslim countries (Roads and Fassihi, 2011).

Yet this earlier statement contradicts more recent messages being disseminated by the Iranian government. A majority of officials have assured the public that they have no plans to shut down internet access, claiming instead that SHOMA and the internet will exist as two separate networks, with the former providing high-speed access to local content and services, and the internet continuing to offer Iranian citizens global connectivity (ITIran, 2012).

The Information Technology Organisation (ITO) has claimed that SHOMA will improve rather than worsen Iranians' browsing experience, as it will enable users to browse local and governmental websites at speeds far higher than they are used to. In this way, it is being framed as a high-speed corridor to access the sites deemed most important (and least controversial) by the government (Tajdin, 2013).

> *Despite what others think, [SHOMA] is not primarily aimed at curbing the global internet but Iran is creating it to secure its own military, banking and sensitive data from the outside world. Iran has fears of an outside cyber-attack like that of Stuxnet [the computer worm developed to attack Iran's nuclear infrastructure], and is trying to protect its sensitive data from being accessible on the world wide web.*
>
> An Iranian IT expert speaking anonymously with The Guardian (Kamali Dehghan, 2012)

Some websites can be accessed on both networks. In these situations the Iranian authorities are encouraging netizens to use SHOMA, as they can more easily monitor its use. In order to attract users to SHOMA the government intends to further decrease the appeal of the global internet. Reporters Without Borders has claimed that the government plans to further throttle connection speeds to the global internet and to increase subscription costs in the hope that subscribing to the faster SHOMA network will become a more attractive prospect (Reporters Without Borders, 2013: 25).

Furthermore, it is also speculated that the authorities have blocked Google and Gmail in an attempt to promote the similar services offered by SHOMA (Reporters Without Borders, 2012b). This process of blocking globally-used websites and applications, and then replicating them domestically is now a frequent occurrence in Iran.

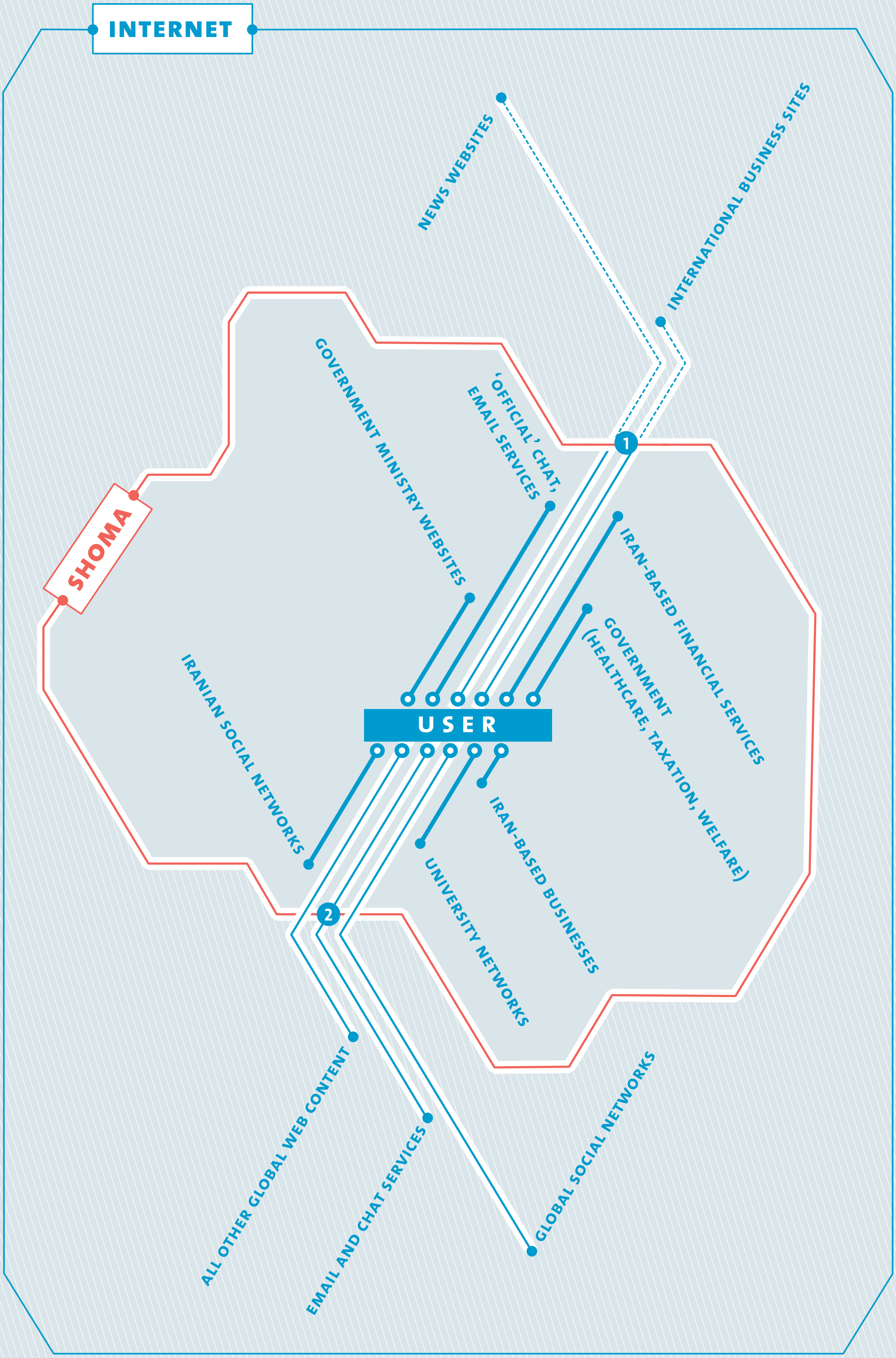

INTERNET
NEWS WEBSITES
INTERNATIONAL BUSINESS SITES
SHOMA
GOVERNMENT MINISTRY WEBSITES
'OFFICIAL' CHAT, EMAIL SERVICES
1
IRAN-BASED FINANCIAL SERVICES
GOVERNMENT (HEALTHCARE, TAXATION, WELFARE)
USER
IRANIAN SOCIAL NETWORKS
IRAN-BASED BUSINESSES
UNIVERSITY NETWORKS
2
ALL OTHER GLOBAL WEB CONTENT
EMAIL AND CHAT SERVICES
GLOBAL SOCIAL NETWORKS

figure 4: SHOMA OVERVIEW

Users can connect to online content via SHOMA or the internet

Authorities plan for SHOMA to be used to access all domestically-hosted content, and the internet for all content hosted outside Iran.

SHOMA

High-speed broadband

Usage of SHOMA is straightforward for the government to monitor and control

Sites hosted on SHOMA include:

- Iran-based businesses
- Iran-based financial services
- eGovernment (healthcare, taxation, welfare)
- Government ministry websites
- University networks
- Iranian social networks
- ‘Official’ chat, email services

Internet

Capped at 128kb for private users

All content accessed via internet connection is filtered according to government restrictions

Sites accessible via internet connections include:

- International business sites
- News websites
- Global social networks
- All other global web content
- Email and chat services

1. Access denied
In times of unrest, the government will be able to completely cut off access to the internet without affecting key services

2. Access granted
Usually, users will be able to access a censored version of the World Wide Web, with speeds capped at 128kb/s

The table below shows just how frequently this is taking place. All major blocked services and social networks have seen at least one Iranian analogue produced, as have a number of services that are still freely accessible (Small Media, 2014b).

Non-Iranian Service	Iranian Service
Facebook (blocked)	Cloob // Facenama
YouTube (blocked)	Aparat
WeChat (blocked)	Dialog
Google Analytics (blocked)	Webgozar
Instagram (partially blocked)	Lenzor
Google Play (partially blocked)	Cafe Bazaar
iTunes Store (previously blocked)	BeepTunes
Firefox (unblocked)	Saina
Google (unblocked)	Parsijoo
App Store (unblocked)	Sibche

Such efforts to develop the range of content and services offered on SHOMA are largely aimed at enticing users onto the new network. Whereas Facebook, Youtube and WeChat are only accessible via VPNs, and therefore function at a snail's pace, the state is now offering a bounty of comparable tools, each of which users can access at high speeds and through legitimate channels - all they need to sacrifice is their privacy.

Ultimately, SHOMA may not threaten the long-term accessibility of the global internet in Iran, but huge concerns remain that it will enable the government to more 'cleanly' throttle internet access during periods of political or social unrest, without crippling crucial SHOMA-based infrastructure and services such as banks, airports, and universities. Although its eventual development may result in lessened frustrations for a large number of Iranian users looking to make use of local and government online services, its emergence will equip the Iranian government with a powerful new tool for smothering political dissent online.

Closing the Net

The Iranian government has demonstrably earned its title as an ‘enemy of the internet’. It has not only worked to arbitrarily censor content that it deems troublesome, but it has made a concerted effort to erode the online security and privacy of its citizens in order to expand its surveillance capabilities.

Nor do these efforts appear to be lessening under the stewardship of the moderate Rouhani administration. Although he and his ministers have made a number of relatively progressive statements relating to internet freedom, hardline elements retain control over many aspects of internet policy making and enforcement. The most effective intervention that Rouhani has made so far in the realm of internet policy has been to act as a roadblock to the ambitions of more conservative elements by vetoing plans to block WhatsApp.

At the same time, efforts to further expand Iran’s capabilities for filtering and controlling internet traffic are continuing apace. The ‘intelligent filtering’ system promises to engage in a far more streamlined and comprehensive form of content filtering than exists at the present time, whereas SHOMA has the potential to fundamentally redefine the relationship between Iran and the World Wide Web, granting the state expanded surveillance capabilities and allowing it to essentially choke off the country’s connection to the World Wide Web in times of crisis.

Though Iranian users have become adept at technological innovation and adaptation in order to stay one step ahead of the state censors, the censorship establishment has also demonstrated a continuing determination to assert their authority over the digital sphere. Given the apparent inability (or unwillingness) of the Rouhani administration to make real concessions in the name of internet freedom, there is little reason to doubt that this national game of cat-and-mouse will continue for a very long time. ◊

References

Arseh Sevom, (2012), "Breaking and Bending Censorship with Walid al-Saqaf", (last accessed: 1/10/2014) available at: http://bit.ly/ArSevomCens

CITNA, (2013), "Rouhani on Network 4: It is undignified for our people to wait so long for information", (last accessed: 1/10/2014) available at: http://bit.ly/RNetPrmse

Elgin, Ben, Vernon Silver and Alan Katz, (2011), "Iranian Police Seizing Dissidents Get Aid Of Western Companies", (last accessed: 1/10/2014) available at: http://bit.ly/IrFrDiss

Esfandiari, Golnaz, (2012), "Iran Announces New Restrictions For Internet Cafes", Radio Free Europe/Radio Liberty, (last accessed: 1/10/2014) available at: http://bit.ly/IRNntcfs

Esfandiari, Golnaz, (2013), "Iran Admits Throttling Internet To "Preserve Calm" During Election", Radio Free Europe/Radio Liberty, (last accessed: 1/10/2014) available at: http://bit.ly/IRthrtle

Fararu, (2014), 'Culture Minister: The filtering of Facebook will be cancelled', (last accessed 1/10/2014) available at: http://bit.ly/Irfafaru

Fars News, (2014a), "CDICC's rulings cannot be overruled / The ICT Minister is incorrect", (last accessed: 1/10/2014) available at: http://bit.ly/frsnwscdicc

Fars News, (2014b), "VPN salesman arrested in Nishapur", (last accessed: 1/10/2014) available at: http://bit.ly/frsnwsvpnar

ICHRI, (2014), "Iran's New Methods of Internet Filtering Put Users At Risk", (last accessed: 1/10/2014) available at: http://bit.ly/ICHRIfil

ISNA, (2013), "Man selling VPNs is arrested", (last accessed: 1/10/2014) available at: http://bit.ly/ISNAvpn

ISNA, (2014), "The results of the latest youth survey have been published", (last accessed: 1/10/2014) available at: http://bit.ly/IrVPNyth

ITIran, (2012), "Separation of Traffic on the Intranet Confirmed", (last accessed: 1/10/2014) available at: http://bit.ly/ITirsptr

ITU, (2012), Recommendation Y.2770 11/12, (last accessed: 1/10/2014) available at: http://bit.ly/ITUrec12

Kamali Dehghan, Saeed, (2012), "Iran clamps down on internet use", The Guardian, (last accessed: 1/10/2014) available at: http://bit.ly/IRclnu

Kelly, Sanja and Sarah Cook, (2011), "Freedom on the Net 2011: A global assessment of Internet and digital media freedom", Freedom House, (last accessed 1/10/2014) available at: http://bit.ly/FrdHse11

Kelly, Sanja, Sarah Cook and Mai Truong, (2012), "Freedom on the Net 2012: A global assessment of Internet and digital media freedom", Freedom House, (last accessed: 1/10/2014) available at: http://bit.ly/FrdHse12

Khabar Online, (2014a), "National Cyber Police Chief: VPNs drive up cost of detecting crime / VPNs will be restricted", (last accessed: 1/10/2014) available at: http://bit.ly/VPNrstr
Khabar Online, (2014b), "The lack of macro filtering policies is problematic / Social networks are being used for spying", (last accessed: 1/10/2014) available at: http://bit.ly/socnetSPY

Khodabakhshi, Leyla, (2014), "Rouhani move over WhatsApp ban reveals Iran power struggle", BBC News, (last accessed: 1/10/2014) available at: http://bit.ly/IRrhniWA

Mashregh News, (2013), "Arrest of seller of internet filters", (last accessed: 1/10/2014) available at: http://bit.ly/IRfltrAR

Mehr News, (2014), "Akhavian's statement on the length of Google sanctions in Iran / People have problems with 'bad filtering'", (last accessed: 1/10/2014) available at: http://bit.ly/BDfiltr

NBC News, (2013), "Iran's President Hassan Rouhani speaks in exclusive interview", (last accessed: 1/10/2014) available at: http://bit.ly/NBCrouhint

Parsons, Christopher, (2011), "Is Iran Now Actually Using Deep Packet Inspection?" (last accessed: 1/10/2014) available at: http://bit.ly/IRdpi

Pourkhasalian, Abbas and Hassan Pouresmail, (2014) "A Review of the Price and Quality of Internet Access in Iran", Islamic Parliament Research Centre, (last accessed: 1/10/2014) available at: http://bit.ly/mjlsINT

Reporters Without Borders, (2012a), "Internet Enemies Report 2012", (last accessed: 1/10/2014) available at: http://bit.ly/RwoB12

Reporters Without Borders, (2012b), "Government blocks Google and Gmail, while promoting National Internet", (last accessed: 1/10/2014) available at: http://bit.ly/RwoB12a

Reporters Without Borders, (2013), "Enemies of the Internet: 2013 Report", (last accessed: 1/10/2014) available at: http://bit.ly/RwoB13

Reuters, (2007), "Iran shuts down 24 cafes in Internet crackdown", (last accessed: 1/10/2014) available at: http://bit.ly/CFEcrkdwn

Schoen, Seth and Eva Galperin, (2011), "Iranian Man-in-the-Middle Attack Against Google Demonstrates Dangerous Weakness of Certificate Authorities", (last accessed: 1/10/2014) available at: http://bit.ly/IrMitMat

Secklow, Steve, (2012), "Special Report: How foreign firms tried to sell spy gear to Iran", (last accessed: 1/10/2014) available at: http://bit.ly/Irspygr

Seifi, Farnaz and Ben Knight, (2012), "Halal Internet' imminent in Iran", Deutsche Welle, (last accessed: 1/10/2014) available at: http://bit.ly/IRhllint

Small Media, (2013a), “Closed Society Meets Open Information”, (last accessed: 1/10/2014) available at: http://bit.ly/IRIWiki

Small Media, (2013b), Iranian Internet Infrastructure and Policy Report March 2013, (last accessed: 1/10/2014) available at: http://bit.ly/IIIPmar13

Small Media, (2013c), Iranian Internet Infrastructure and Policy Report June 2013, (last accessed: 1/10/2014) available at: http://bit.ly/IIIPjn13

Small Media, (2014a), Iranian Internet Infrastructure and Policy Report March 2014, (last accessed: 1/10/2014) available at: http://bit.ly/IIIPmr14

Small Media, (2014b), Iranian Internet Infrastructure and Policy Report July 2014, (last accessed: 1/10/2014) available at: http://bit.ly/IIPJl14

Roads, Christopher and Farnaz Fassihi, (2011), “Iran Vows to Unplug Internet”, (last accessed: 1/10/2014) available at: http://bit.ly/IRunplug

Tajdin, Behrang, (2013), “Will Iran’s national internet mean no world wide web?” BBC News, (last accessed: 1/10/2014) available at: http://bit.ly/bbcSHOMA

Tasnim News, (2014a), “Vaezi: CDICC cannot overrule final decision of the President”, (last accessed: 1/10/2014) available at: http://bit.ly/IrVaez

Tasnim News, (2014b), “Illegal proxy salesman arrested in Kerman”, (last accessed: 1/10/2014) available at: http://bit.ly/KrmnVPN

The National, (2014), “Iran’s internet censorship not in country’s interest: Rouhani”, (last accessed 1/10/2014) available at: http://bit.ly/NatRouCen

Small Media

Editors
Bronwen Robertson
James Marchant

Contributors
Kyle Bowen
James Marchant

Research Assistants
Benjamin Graff
Marine Strauss
Raha Zahedpour

Graphic Designers
Isabel Beard
Richard Kahwagi

Arab Media Report

Contributors
Antonello Sacchetti
Valeria Spinelli