Internet in Chains

The Front Line of State Repression in Iran

November 2014

INTERNATIONAL CAMPAIGN FOR HUMAN RIGHTS IN IRAN

Internet in Chains
The Front Line of State Repression in Iran

Internet in Chains

The Front Line of State Repression in Iran

November 2014

INTERNATIONAL CAMPAIGN FOR HUMAN RIGHTS IN IRAN

www.iranhumanrights.org

About Us

The International Campaign for Human Rights in Iran is an independent, nonpartisan, nonprofit organization dedicated to the protection and promotion of human rights in Iran.

The Campaign investigates and documents rights violations occurring throughout Iran, relying on first-hand accounts to expose abuses that would otherwise go unreported. We bring these violations to the attention of the international community through news articles, briefings, in-depth reports, podcasts, and videos, and work to build support for human rights inside Iran as well. The Campaign engages in intensive outreach and international advocacy aimed at defending the fundamental rights and freedoms of the Iranian people and holding the Iranian government accountable to its human rights obligations.

Table of Contents

Executive Summary

Censorship and state control over the Internet in Iran is changing: it is becoming more systemic and less detectable, posing an ever-greater threat to Iranian users. Increasingly, the state is focusing on developing the technological infrastructure to effectively control access to the Internet inside Iran and covertly monitor its use. In effect, the state is attempting to create a wall around the Internet, and to serve as its sole gatekeeper, allowing or denying entry at will and gaining full access to the accounts of those whom it allows in.

The intensification of state efforts reflects the fact that the Internet has increasingly emerged as one of the central battlegrounds between hardliners anxious to control all expression and access to information in Iran, and the majority of the population, who voiced their desire for greater openness and freedom with the election of the centrist Hassan Rouhani to the presidency in June 2013.[1]

Keenly aware of the Iranian citizenry's embrace of the Internet, hardliners ensconced in the judicial, intelligence and security arms of the state and backed by Supreme Leader Ali Khamenei have ensured that the country's Internet policies remain under their control, immune from electoral politics.

The highest body responsible for overseeing the Internet is the Supreme Cyberspace Council.[2] In charge of general policies, it was formed in 2012 under the direct orders of Khamenei, who views the Internet as a corrupting influence that must be strictly censored and controlled.

The body that monitors cyberspace and is responsible for indexing the websites and mobile applications that are to be blocked by the Telecommunications Ministry, is the Working Group to Determine Instances of Criminal Content on the Internet.[3] Formed in 2009, it works under the supervision of the Prosecutor General, and has 13 members. Six of these are members of the president's cabinet. The remaining seven are comprised of representatives of the Intelligence Ministry, Guidance Ministry, the Islamic Republic of Iran Broadcasting (IRIB) agency, and other state organizations who are vetted and controlled by Khamenei. The members representing the elected administration are thus a permanent minority and not able to have a definitive impact on the decisions of the group.

The Working Group has criminalized content that is supposedly contrary to "public chastity and morality," "sacred Islamic principles," "security and public peace," and "government officials and public institutions." These highly subjective and potentially all-encompassing determinations have given the hardliners free reign to take sweeping action based on their own interpretations and political proclivities.

The state's efforts to achieve control over digital communications in Iran have focused on three main areas. First, authorities are developing the technical infrastructure that will give various state agencies full control over Internet access inside Iran. This includes developing the Iranian National Information Network (or "National Internet"), which will allow the state to be the sole "gatekeeper" to the Internet inside Iran; providing government-issued SSL security certificates, which will enable undetected government access into accounts; and developing a national browser and operating system, which will ensure use of the government SSL certificates. Second, authorities are continuing their filtering activities, with a focus on mobile phone applications, which have become an increasingly central platform for Internet use in Iran. Third, hardliners in the Judiciary and the intelligence and security services are strengthening the state's ability to target and prosecute online activists.

The development of Iran's National Information Network will exponentially increase the state's control over Internet access and use in Iran. Planning for the National Internet began in 2006, but it has yet to be fully implemented and it is not clear when it will become operational. According to the government's five-year development plan (2011-2015, or 1390-1394 in the Persian calendar), the network is designated to be up and running by early 2016, but the project has experienced repeated delays.[4] Yet work on the project has continued steadily and once it is fully implemented, all Internet access in Iran will take place through channels accessible to the state, state agencies will have access to all communications inside Iran on the National Internet, the authorities will be able to cut off access to the global Internet at will, and they will also be able to deny or limit access by Internet users abroad to content in Iran's domestic Network.

In order to launch the National Information Network, the central government is setting up "National Data Centers" in Tehran and other cities across Iran, where the various telecommunications and storage systems will be housed.[5] This will provide authorities with full access to the servers used by—and thus any content flowing across—the National Network.

Government-issued SSL security certificates will further facilitate government control over and access to Internet communications in Iran.[6] SSL certificates ensure that the connection used in any Internet transmission is encrypted and thus secure. When they are issued by a legitimate source, they do indeed ensure security. The government is discouraging the use of valid certificates (by occasionally demonstrating their capability to block international SSL certificates, as was done during the disputed 2009 presidential elections, when Iranian users were prevented secure access to sites such as Gmail, Facebook, and Twitter), and developing its own national SSL security certificates, which will give the user the illusion of security online, but which will actually give the government full access to the content.

SSL certificates that are issued by the Iranian government, non-governmental or private sector organizations controlled by the state, or Iranian security or military agencies will allow those (issuing) organizations to have full access to the online activities of the users.

SSL certificates that are issued by the Iranian government, non-governmental or private sector organizations controlled by the state, or Iranian security or military agencies will allow those (issuing) organizations to have full access to the online activities of the users. Critically, it will become difficult for users to recognize whether they are using an Iranian government SSL certificate or an international one; while most operating systems and browsers will recognize and alert the user that a SSL certificate is not from a trusted source, if an untrusted SSL certificate is used by enough (unsuspecting) users, these certificates become “trusted” certificates which means that they are no longer tagged as untrusted, eventually leading to “root” certification, which means they are considered completely safe. Achieving root certification for the national certificates through their repeated use is the strategy pursued by the authorities.

The government has employed two means to promote widespread usage of its SSL certificates: it has built the certificates into the national Iranian web browser, Saina,[7] and into the national operating system, Zamin,[8] which are both provided by state agencies. The browser and operating system will not recognize Iran’s SSL certificates as “untrusted,” facilitating their steady use until they gain root certification.

In order to ensure widespread use of the national browser and operating system, the government banned the use of the Windows operating system in state offices in 2013, specifying a six-month implementation period in which all executive branch computers must switch their software from Microsoft to Linux, which would carry the new systems.[9] However, the logistics of such a transition are onerous and to date there has been no report regarding its progress. Iranian officials had also promised to launch the Zamin (Earth) national operating system with cloud data processing compatibility and an operating system for hand-held devices by spring 2013, but implementation has been behind schedule on this as well.[10]

Nevertheless, these initiatives reveal a concerted effort by the authorities to ensure that all Internet communications take place in a state-controlled environment. The successful launch of such a system, in the absence of a legal framework to protect individual privacy, will mean that Internet users in Iran will be sharing their information with the country's security, intelligence, and judicial agencies.

The successful launch of the National Internet, in the absence of a legal framework to protect individual privacy, will mean that Internet users in Iran will be sharing their information with the country's security, intelligence, and judicial agencies.

In parallel with the development of the National Information Network, the authorities have also tried to limit Iranian users' access to the global Internet. One of the principal ways that Iranians have been able to maintain access to the Internet has been through the use of Virtual Private Networks (VPNs). These allow users to circumvent government filters by providing encrypted links to networks based abroad, effectively enabling a computer to function as if it is based in another country and thus able to directly connect to the global Internet. As a result, the authorities have increasingly moved to shut down VPN ports. In March 2013, Mehdi Akhavan Behabadi, the director of the Supreme Cyberspace Council, announced the closure of VPN ports, and since then a number of ports have been shut down.[11] Success on this front, however, has been intermittent; frequently users are able to establish new VPN ports to replace those that have been lost.

In addition, Behabadi called for their replacement with "legal VPNs," and in recent months officials have encouraged the use of VPNs provided by the government.[12] Unsurprisingly, this latter effort has met with little success; there has been scant interest in using government-issued VPNs where filtered sites remain filtered, since the purpose of using VPNs is to access filtered sites.

Along with blocking VPNs, government agencies have also permanently blocked access to popular filter-breaker services (Internet censorship circumvention tools) such as Psiphon, TOR, and Browsec.[13]

While the development of this new infrastructure has been central to the state's current efforts, filtering has not been ignored. Previously, the authorities focused on the filtering of websites. While there is no official information regarding the number of filtered sites, in 2008, the last time an official statement regarding filtered sites was made, Abdolsamad Khorramabadi, a judiciary adviser at the time, stated that five million websites had been filtered.[14] However, filtering has now also been applied towards mobile applications, in recognition of the increasing primacy of mobile devices in Iran.

> ***In 2008, the last time an official statement regarding filtered sites was made, Abdolsamad Khorramabadi, a judiciary adviser at the time, stated that five million websites had been filtered.***

In the past six months, the Working Group to Determine Instances of Criminal Content on the Internet has ordered the blocking of mobile applications such as WeChat, WhatsApp, Tango, and Viber. While WeChat, filtered in January 2014, remained blocked at the time of this writing, WhatsApp, widely used in Iran, was eventually unblocked at the request of President Rouhani, reflecting the tug of war between the administration and hardliners over the Internet.[15] Viber and Instagram have been unblocked as well.

In addition to these areas, the authorities have aggressively pursued the prosecution of online activists. With the government fully in control of all print and broadcast media, the Internet has emerged as the principal forum where independent and dissident voices can be heard. Recognizing this, the Iranian Cyber Police, also known as FATA, was established in 2011 as the cybercrime unit of the Iranian national police force.[16] One of FATA's activities is to monitor the activities of civil and political activists, and pursue citizens who express dissenting views online. FATA's arrest of Sattar Beheshti, the 35-year-old blogger who died under torture while in FATA's custody in November 2012, is indicative of the vehemence with which they intend to stamp out online dissent.[17]

The cyber police have also pressured Internet providers to provide them with evidence they can use to pursue online activists. One company, Bayan, disclosed publicly that FATA had tried to illegally obtain information about one of its online customers (which the company resisted), and published copies of four letters exchanged with FATA, including one in April 2014 in which FATA demanded that the company immediately hand over the activity records of a user for further investigation.[18]

Iran also relies on its Cyber Army, a unit of the Revolutionary Guards, whose central role is to monitor, hack, and bring down any (domestic or foreign) website that is perceived to pose a potential challenge to the authority of the state.[19] The opaque nature of the Cyber Army's reporting structure and organization is critical to its ability to function extra-judicially, carrying out disabling attacks on websites and removing these voices of perceived dissent, without court order or any responsible official that a citizen or organization can point to, question, or hold accountable.

> ***Iran relies on its Cyber Army, a unit of the Revolutionary Guards, whose central role is to monitor, hack, and bring down any (domestic or foreign) website that is perceived to pose a potential challenge to the authority of the state.***

Other state organizations have pursued those active in cyberspace as well. The December 2013 arrest by units of the Revolutionary Guard of members of the Narenji (Orange) website staff reflects the intensification of these efforts currently underway.[20] The Narenji site was focused on the latest developments in technology tools. In June 2014, eleven information technology professionals working for the Narenji website were sentenced to between one and eleven years imprisonment. The sentencing of eight young Facebook users in July 2014 to prison terms that ranged from 8 to 21 years for content posted on their Facebook pages, even though they have since been released on bail, reflects the Judiciary's active collusion in the repression of social media users, as well.

Taken together then, the development of the National Internet, the filtering of mobile applications and websites, and the intensified prosecution of online activists, indicate that the state has significantly increased intent—and capability—to stamp out online dissent.

Officials in Iran have claimed their National Internet is aimed at delivering faster speeds, cheaper service, and greater online security to Iranian users, as well as facilitating Iranians' access to tools and services that are unavailable to them due to the international sanctions against the country. Yet these alleged benefits, even if they were accurate, are meaningless in the absence of a structured legal framework that respects the rights and privacy of citizens. The principal result of these activities has been to make Iranian citizens profoundly vulnerable to security and judicial institutions that seek to gather information about online communications in order to harass, control, and detain users.

While the June 2013 election of Hassan Rouhani ushered in hopes for a change in the government's Internet policies, the reality that state control over the Internet is increasing is a sober reminder that key centers of power in Iran remain committed to online repression.

> ***Rouhani has rhetorically promoted Internet freedom; it is part and parcel of his overriding policy objective, namely, the economic revitalization and modernization of the country.***

To be sure, Rouhani has rhetorically promoted Internet freedom; it is part and parcel of his overriding policy objective, namely, the economic revitalization and modernization of the country. Moreover, he has had some notable achievements. His unblocking of the WhatsApp mobile application in May 2014, and his granting of licenses to provide 3G and 4G services in the country, were both significant. Indeed, hardliners had long railed against fast Internet speeds (and the access to content not controlled by the State that such speeds would allow), and had relied on the practice of slowing down Internet speeds to the point where its use was rendered effectively impossible.

Nevertheless, such support has translated into relatively few tangible policies, and hardliners in the intelligence, security and judicial branches and supported by Khamenei have been able to pursue their intensified control over the Internet.

It is imperative that the evolving nature of this control—and the dangers it poses, especially to those engaged in social or political activism—be revealed and understood. Civil society groups inside and outside Iran should continue to urge the Rouhani administration to honor its pledges of greater Internet freedom. Yet until the domestic context in Iran allows positive change in this regard, the international community must make every effort to alert Iranian civil society to existing and emerging vulnerabilities online, assist them in the development of technologies and tools that will counter such repression, and publicly defend the universal right to freedom of expression and access to information in Iran.

Introduction

The Internet in Iran has increasingly become one of the central battlegrounds in the struggle between the state and its continued ability to control information and expression inside the country, and the citizenry, who desire free expression and engagement with the modern world.

The stakes are high. For the government, or, more accurately, the hardliners who control key centers of power in the country such as the judicial, intelligence, and security services, restricting the population to its own world view is seen as an existential issue; loss of control over the narrative risks loss of their political power. For the citizenry, who resoundingly demonstrated their desire for greater rights and freedom with their election of the centrist president Hassan Rouhani in June 2013, unrestricted access to the Internet is a requirement for modern literacy and relevance.

Each side in this struggle is strong. Iran is one of the most censored countries in the world. The government already controls all print and broadcast media, and, given the centrality of digital communication, has increasingly focused its attention on controlling online content as well. It blocks millions of websites, monitors and hacks into private citizens' online communications, is intensifying its development of the country's National Intranet and other tools that will give the authorities control over Internet access inside Iran, criminalizes the use of social media, and targets IT and social media professionals for prosecution. It is considered second only to China in the sophistication of its Internet filtering and monitoring technologies. It is also ruthless in the persecution of those it feels have crossed red lines; it routinely arrests and detains individuals for online activities, and the murder, under torture by cyber police interrogators, of the blogger Sattar Beheshti within a few days of his detainment in November 2012, reflects the perceived stakes in this battle.[21]

The population also has its strengths. It is young—over 60% of the population is under 30—and educated—85% of the population is literate, well above the regional average. It is also, increasingly, online: some 42 million people, or 55% of the population, are connected to the Internet. Its population has proven to be technologically savvy in finding ways to circumvent the state's digital censorship, forcing the authorities to play an endless game of cat and mouse in which they must address each new censorship circumvention tool as it arises.

The struggle has intensified since Rouhani's election. Rising expectations on the part of the population that the electoral mandate delivered to Rouhani would result in greater openness have clashed with hardline factions anxious to re-assert their primacy. Development of Internet filtering and monitoring tools has accelerated and arrests of IT professionals have increased. The Rouhani administration has pushed back some–a statement defending the need for open Internet access is made, a block on an application is removed–but it has largely refrained from taking the gloves off, focusing instead on its foreign policy objectives, particularly maintaining forward momentum on the P5+1 nuclear negotiations.

The Rouhani administration has pushed back some–a statement defending the need for open Internet access is made, a block on an application is removed–but it has largely refrained from taking the gloves off, focusing instead on its foreign policy objectives, particularly maintaining forward momentum on the P5+1 nuclear negotiations.

In this report by the International Campaign for Human Rights in Iran, the extent and nature of this intensifying digital censorship and control is comprehensively reviewed. The report presents a detailed overview of the policies, programs, institutional structure, and technological tools, methods, and capabilities of Iranian online control. It also analyzes the broader domestic political context in which this censorship is being carried out, examining the forces pushing for and against online censorship, and assesses the impact of this censorship on Iranian users, particularly individuals who use the Internet as a means to conduct social, political, and human rights activism.

The report is based on in-depth analysis of online data, extensive interviews with Iranian information technology professionals and users inside the country, public record statements by Iranian officials, and official government policies regarding Internet use in Iran.

The central conclusion is disturbing: not only is Iranian online censorship and control intensifying, its nature is changing dramatically and in ways that pose grave dangers to Iranian Internet users—especially those that use the Internet for political or social activism. In addition to its long-standing filtering and blocking activities, the government is increasingly focusing on developing and employing technologically sophisticated means to control access to the Internet inside Iran, and to monitor, undetected by the user, online communications. This is a far more insidious and dangerous form of repression, rendering the content of online communications fully accessible to the authorities. It profoundly increases the vulnerability of Internet users as it will allow the authorities to identify and target individuals at will. This could be crippling to Iranian civil society, encouraging self-censorship and preventing the kind of online communication and information sharing critically needed by journalists, students, activists, human rights defenders, and other members of Iranian civil society.

It is imperative that the international community and Iranian citizens understand the evolving nature of Internet control inside Iran, so that tools and strategies can be developed to counter such activities. This report by the Campaign is intended to contribute to that effort.

Internet Censorship and Filtering

The Internet first became available in Iran in 1993 with the start of dial-up services.[22] Over the next few years, there were no clear guidelines for filtering sites and filtering remained relatively limited, with only intermittent instances of blocking of political or dissident sites, as the authorities did not yet realize the Internet's potential as a communication tool.

Gradually, however, as use of the Internet began to grow in Iran and authorities began to realize its potential power, the government began to focus more on its censure. During the early years of the reformist Khatami presidency, (1997-2005), there was a relative flourishing of the press. This triggered a backlash by more conservative forces in the government, and the clamping down on print media was met with a corresponding increase in online blogs focused on political and social activism, which alerted authorities to the increasing role of the Internet.

In recognition of the growing role of the Internet, in June 2001, Khamenei decided that the Supreme Cultural Revolution Council, a body of officials originally formed by Ayatollah Khomeini to rule on major social and cultural issues in the country, would be in charge of determining acceptable Internet content, and it issued general guidelines for the Internet that were aimed at stamping out any kind of expression deemed critical of the government or the country's religious establishment.[23] Gradually, as use of the Internet increased, this Council ordered more systematic filters and blocks on websites, and one year later, in 2002, the Iranian Parliament passed a law that determined guidelines for identifying criminal Internet activities. The Committee to Determine Illegal Websites was formed a year later, laying the institutional and legislative groundwork for the authorities to prosecute individuals for their online activities.[24] For this purpose a branch for Internet affairs was established at the Prosecutor's Office in Tehran in 2003.[25]

During Khatami's second term, the filtering of websites and clamping down on bloggers intensified. The arrest in 2003 of the journalist Sina Motalebi[26] for his personal political blog, "Webgard," and the 2004 "Bloggers Case"[27] in which a group of journalists and bloggers were imprisoned for their online writings, marked a turning point, signaling that the state would focus considerable efforts on the strict censorship of the Internet and prosecute bloggers for online activity deemed transgressive.

With the election of the hardline Ahmadinejad in 2005, restrictions on free speech and access to information intensified. In August 2006, Ahmadinejad's administration issued a directive requiring all Internet sites to be registered at the Culture and Islamic Guidance Ministry.[28] After the disputed 2009 presidential election and the violent suppression of peaceful protests in its wake, the stamping out of any dissent—particularly in online forums, which had been central to the mobilization and organization of the 2009 protests—became a priority for the government. In 2009, the Majlis passed the Computer Crimes Law and established the Working Group to Determine Instances of Criminal Content on the Internet, charged with supervising cyberspace activities, determining sites with "criminal" content, and investigating complaints from the public.[29]

■ Members of the Working Group to Determine Instances of Criminal Content on the Internet

- Prosecutor General (head of the group)
- Minister of Intelligence, or his representative
- Minister of Culture and Islamic Guidance, or his representative
- Minister of Justice, or his representative
- Minister of Telecommunications and Information Technology, or his representative
- Minister of Science, Research and Technology, or his representative
- Minister of Education, or his representative
- Chief of Police
- An information technology expert chosen by the Industries Commission of the Majlis
- A member of the Majlis Justice and Law Commission approved by the Majlis
- Head of the Islamic Promotion Organization
- Head of Islamic Republic of Iran Broadcasting (IRIB)
- A representative from the Supreme Cultural Revolution Council's secretariat

The Working Group declared the following as criminal content, based on Article 21 of the Computer Crimes Law and related articles in the Islamic Penal Code, the Press Law, and regulations passed by the Supreme National Security Law: content against public chastity and morality; content against sacred Islamic principles; content against public security and welfare; content against government and public officials and agencies; content intended for Internet crimes; content that incites, encourages, or invites people to commit crimes; criminal audio and visual content and copyright issues; and criminal content related to Majlis [the Iranian parliament] elections or presidential elections.[30] These broad and subjective determinations provided authorities with free reign to impose sweeping limitations on permissible Internet content.

The Working Group, under the supervision of the Prosecutor General, thus became the principal, though not exclusive, state body charged with indexing the specific Internet sites to be blocked. The Group has 13 members, including six representing the executive branch and two from the Judiciary.

> ***The institutional structure of the Group (and indeed of all state bodies charged with formulating Internet policy in Iran) is designed to immunize it from democratic politics.***

The institutional structure of the Group (and indeed of all state bodies charged with formulating Internet policy in Iran) is designed to immunize it from democratic politics. The six members representing the executive branch are a permanent minority; even if all the administration representatives opposed filtering a certain site, they would not be able to defeat a united non-administration faction within the Group.

According to the Computer Crimes Law, members of the Working Group must meet every two weeks to discuss and vote on which Internet sites should be blocked. After determining the sites and applications to be filtered, the list of sites is sent from the Prosecutor General's Office to the Telecommunications Company of Iran, the Data Communication Services Company, and other related agencies.

■ **Institutional representatives of the Supreme Cyberspace Council**

- President (head of the Council)
- Speaker of the Majlis (Parliament)
- Judiciary Chief
- Head of the Islamic Republic of Iran Broadcasting (IRIB)
- Secretary and Head of the National Cyberspace Center
- Minister of Telecommunications and Information Technology
- Minister of Culture and Islamic Guidance
- Minister of Science, Research and Technology
- Minister of Intelligence
- Head of Majlis Culture Commission
- Head of Islamic Promotion Organization
- Commander in Chief of the Islamic Revolutionary Guards
- Chief of Police
- Prosecutor General

However, decisions regarding filtering are made by more than one agency. In addition to the Working Group, the Supreme Cyberspace Council was established in 2012 under the orders of Khamenei, reflecting the growing importance given to filtering by the Islamic Republic's most senior authorities.[31] The Supreme Cyberspace Council is the highest authority responsible for general policy regarding cyberspace. The members of the Council are composed of two types: institutional representatives and appointed individuals.

While the Supreme Cyberspace Council sets general policies for the Working Group to Determine Instances of Criminal Content, it also creates a list of sites that are to be blocked based on "social unsuitability," "contradiction to Islamic principles," "threats to national security," and any site that promotes ways to circumvent Internet filters. Most members of the two bodies are in fact the same.

■ **Appointed individuals of the Supreme Cyberspace Council**

- Hamid Shahriari
- Seyed Javad Mazloumi
- Masoud Abu Talebi
- Kamyar Saghafi
- Rasoul Jalili
- Mohammad Sarafraz
- Alireza Shahmirzaie
- Mehdi Akhavan Behabadi

Websites can also be tagged for blocking by other organizations. For example, some sites are filtered on the direct orders of the Judiciary. The Revolutionary Guard-affiliated Islamic Republic of Iran Cyber Army hacks and brings down the websites of government critics, and the Iranian Cyber Police, known as FATA, also has an active role in filtering sites. Most recently, the Ministry of Culture and Islamic Guidance has also been directly ordering the filtering of sites.

Filtering the Internet, then, gradually became over these two decades a highly focused and institutionally formalized state priority, supported at the highest levels of government and insulated from electoral politics. In 2006, the *Guardian* newspaper estimated that after China, Iran had the highest number of filtered websites in the world.[32] Abdolsamad Khorramabadi, who at the time was an adviser at the Judiciary, told Mehr news agency on November 19, 2008, that five million sites had been filtered in response to "enemies who take advantage of the Internet to attack our religious identity."[33] He claimed that the Internet had a destructive impact on social, political, economic, and moral aspects of society and added, "It would benefit us to reduce the damaging impact of the Internet by educating society, especially pre-university and university students, and strengthening the foundations of family, establishing a cyber police force, and passing laws to fight Internet crime."

Overall, the Iranian government has been quite opaque about its filtering activities. It releases no official data or statistics, and has aggressively stopped independent organizations from ascertaining information on the number of sites that have been filtered, let alone a definitive listing of which sites have been blocked. The case of the company FilterShod.ir is indicative of the government's attitude toward the public disclosure of its filtering activities.

FilterShod.ir was a project of the privately owned Iran-based LifeWeb company. Launched in May 2013, it gathered and published daily information on which websites the Iranian government was filtering, and published weekly and monthly reports detailing the sites the Iranian government had blocked or unblocked. Yet less than a year after its launching, the authorities closed down the project.

It was never known which security service shuttered the site. Up until its closure on February 10, 2014, it had registered 40,955 filtered sites in its ten months of existence. It was clear that FilterShod had crossed a red line for the Iranian government. For the first time since the Internet came to Iran, a private company had attempted to monitor the government's filtering activities. FilterShod's shuttering reflects how important the opacity of the filtering process is to the authorities—which sites are blocked, how many sites are blocked, and the filtering process itself—all remain undisclosed. The authorities clearly do not want the data tracked or the filtering process understood.

The Iranian government has aggressively stopped independent organizations from ascertaining information on the number of sites that have been filtered, let alone allowing a definitive listing of which sites have been blocked.

At present, the authorities have devoted an increasing amount of attention to also filtering mobile applications. This policy has been most pronounced during the last year and reflects the increasing primacy of mobile devices such as smartphones and tablets in digital communications in Iran.

In December 2013, WeChat, a popular mobile communication service among Iranians, became the first mobile application to be filtered on orders of the Working Group to Determine Instances of Criminal Content. A wave of mobile application filtering actions continued over the next few months, and Viber, Tango, and WhatsApp were also disabled.

Abdolsamad Khorramabadi, secretary of the Working Group to Determine Instances of Criminal Content said in an interview with the ISNA news agency on April 4, 2014, that these applications would have been blocked earlier but action was postponed until the development of national mobile applications.[34] And in fact, the Iranian government has moved forward aggressively to develop its own national versions of mobile applications. For example, the country is developing Zoobi, a localized chat software designed to replace the popular mobile application Viber. The Daneshjoo News Agency quoted Mohsen Torabi, Project Manager for Zoobi, who said the application will be ready for utilization by Android users in November 2014.[35]

The sequence of events in the blocking of WhatsApp, a mobile application widely used in Iran, was significant in that it revealed the continued tug of war between hardliners and the Rouhani administration over the Internet. After the February 19, 2014, announcement by Facebook that it had purchased WhatsApp, the Working Group to Determine Instances of Criminal Content ordered (on May 5, 2014) WhatsApp to be blocked. The next day, Telecommunications Minister Mahmoud Vaezi announced that Rouhani had personally ordered the block on WhatsApp to be removed.[36] Abdolsamad Khorramabadi, a member of the Working Group strongly objected to Rouhani's action, and said, "Essentially the president cannot prevent actions taken by the Working Group."[37] On May 19, 2014, Judiciary Spokesman Mohsen Ejei weighed in, stating, "The Telecommunications Minister has acted against the law and should be answerable for this action."[38] Yet on June 18, 2014, a member of the Working Group said in an interview with the Mehr News Agency, "In light of the President's concern…members of the Working Group took another vote and decided that the filtering of WhatsApp be stopped and we have no plans at present to block any mobile-based social networks."[39] He added that Instagram would also be unblocked. Viber was eventually unblocked as well. (WeChat remained blocked at the time of this report's publication.) Thus WhatsApp was subsequently unblocked by the authority of President Rouhani, in the face of explicit opposition by hardliners.

Rouhani's Minister of Telecommunications has expressed opposition to blocking VoIP (Voice over Internet Protocol), the tools and technology that enable text, voice, and video transfers over mobile phones and tablets, on the grounds that there are simply too many Iranians using the service. Yet Khorramabadi, in an interview with ISNA news agency on April 4, 2014, asserted that mobile apps such as Tango, Viber and WeChat have the ability to exchange intelligence about the country and "collect and analyze information for foreigners," a view widely held by hardliners in the government.[40]

As the debate over filtering mobile applications continues, the head of the mobile systems division of the Digital Media Center has opened a new front, stating that all firms and individuals must now have permits to distribute mobile applications. That this is not required of other software indicates the authorities' growing fear of mobile-based applications. Amir Mirsayyah, head of the mobile systems division of the Digital Media Center, justified the permit requirement at Iran's Sixth Web and Mobile Festival on February 19, 2014, by stating such measures were needed to protect mobile application copyrights.[41] Given the lack of such a requirement for other software, and the fact that the national browser developed by Iran (Saina) is itself a copy of Firefox, such claims are highly suspect.

The National Information Network (National Internet)

□ HISTORY

While the state thus devoted considerable resources and institutional capacity to filtering the Internet, a new dimension began during the Ahmadinejad presidency (2005-2013) regarding Iran's approach to the Internet. Namely, the state decided to develop a national infrastructure that would give the authorities full control over all access to the Internet, as well as the ability to monitor all content that flowed across this national infrastructure.

In 2006, Telecommunications Minister Mohammad Soleymani announced that a "National Information Network," more commonly known as the National Internet, would be launched in two or three years.[42] This Network would create a domestic, government-controlled Intranet, in which the state would decide all content and access. In effect, the National Internet would create a locked wall around the Internet for users inside Iran, with the government as the sole key holder. Needless to say, as sole holder of the key, the government would have full access to the content of any account.

Publicly, the government bills the National Internet as a means to "increase Internet speed and security inside the country."[43] The government also argues the National Internet is needed due to sanctions against the country. While exports of personal communications tools and services to Iran are now allowed, financial transactions remain difficult due to banking sanctions, and Iranians are still blocked from making purchases from many companies such as Apple, Microsoft and other applications stores. They have to use third parties to access them, which security experts discourage as it increases the risk of malware infections, and are also more frequently targeted by online scams that fraudulently sell banned services.

Despite numerous promises, completion dates have been postponed many times. Based on the current five-year development plan (2011-2015, or in the Persian calendar, 1390-1394), the National Internet is to be completed by the end of winter 2016. According to Article 46 of the five-year plan, "The country's National Information Network should be an IP-based Internet supported by data centers that are completely undetectable and impenetrable by foreign sources and allows the creation of private, secure Intranet networks.[44] This definition of the National Network was solidified in the Supreme Cyberspace Council's meeting on December 24, 2013.

The first phase of the National Internet was originally planned for implementation in September 2012, with the separation of Internet and Intranet networks (making the National Network independent of the global Internet). The second phase, originally due by the end of March 2014, would see the hosting of all websites transferred inside the country (in other words, the storage of all the content on the National Internet would be on servers that are physically inside Iran). In the third phase, planned for implementation by 2016, the National Internet would be managed inside the country, exclusively utilizing Iranian software and applications so that foreign software would no longer be used in Iran.

As none of these phases have, as of yet, been fully implemented, the establishment of the National Internet is clearly behind schedule. This is due primarily to a number of technical and logistical difficulties in its development—as well as political infighting between hardliners anxious to push forward its implementation, and more moderate forces, primarily within the Rouhani administration, who see Internet freedom as integral to their overriding goal of economic modernization and revitalization, and have control over budgetary allocations and technical implementation. Iranian officials have publicly blamed delays in the project on the international sanctions regime tied to the country's nuclear program.[45]

Nevertheless, work on the National Internet's development and implementation continues, reflecting a worldview, dominant among hardline authorities who maintain significant power bases in the intelligence, judicial and security apparatuses, in which any non-state-controlled source of information is seen as suspect, if not treasonous. In a typical remark, Police Chief General Ahmadi Moghaddam described Google's search engine as a "spying tool" against users in a January 20, 2012, interview with the Mehr news agency, and stated, "The National Internet can facilitate protecting the people's security and information. Today, South Korea is also using a national Internet for its domestic and foreign communications. I believe the National Internet can be a major step towards protecting the country."[46]

The establishment of the National Internet is clearly behind schedule. This is due primarily to a number of technical and logistical difficulties in its development—as well as political infighting.

□ NATIONAL DATA CENTERS

The National Data Centers are one of the most important infrastructure components of the National Information Network. These Centers will be set up in Tehran and other cities across the country, and will house the various telecommunications and storage systems used by the Network and process all the information flowing across the Network. Critically, the Centers will provide the authorities with full access to the servers used by—and thus any content flowing across—the National Network.

In order to entice Internet providers and Web hosting companies in Iran to store their data in the National Data Centers (as opposed to private firms outside the country such as Google, Microsoft or Apple), the government is increasing the bandwidth of the Centers and thus the speed in which they can store and process information. Mahmoud Khosravi, managing director of the Telecommunication Infrastructure Company, stated, "Previously the network consisted of a 43 GB Cisco system but now it is capable of handling 470 GBs."[47] In a perhaps unintentional admission of the uphill battle the government is facing in convincing users of the "benefits" of the Centers, Khosravi continued, "Of course this network is like a new highway that might have only four cars moving on it and so we are trying to encourage operators to use this completely unbreakable network."[48]

□ NATIONAL SSL CERTIFICATES

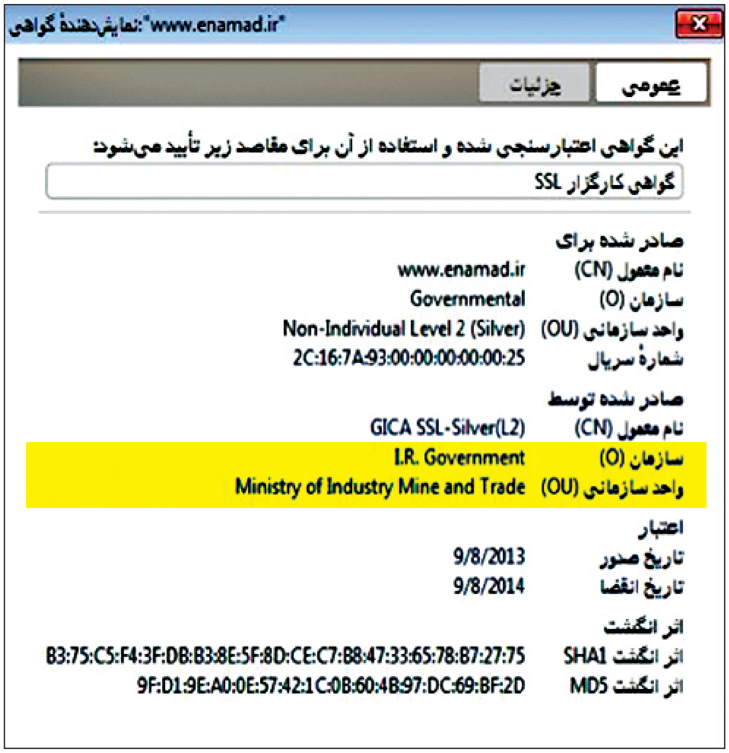
National (government-issued) SSL security certificates are also a central component of Iran's National Internet. SSL certificates ensure that the connection used in any Internet transmission is encrypted and thus secure. When they are issued by a legitimate source, they do indeed ensure security. The government is discouraging the use of valid certificates (by occasionally demonstrating their capability to block international SSL certificates, as was done during the disputed 2009 presidential elections, when Iranian users were prevented secure access to sites such as Gmail, Facebook and Twitter), and developing its own national SSL security certificates.

SSL certificates that are issued by the Iranian government, non-government or private sector organizations controlled by the state, or Iranian security or military agencies will allow those (issuing) organizations to have full access to the online activities of the users. Critically, it will become difficult for users to recognize whether they are using an Iranian government SSL certificate or an international one; while most operating systems and browsers will recognize and alert the user that a SSL certificate is not from a trusted source, if an untrusted SSL certificate is used by enough (unsuspecting) users, these certificates become "trusted" certificates, and are no longer tagged as untrusted. Over time, the process leads to the "root" certification of the SSL certificates, which means they are considered safe.

The National Data Centers will provide the authorities with full access to the servers used by—and thus any content flowing across—the National Network.

On November 23, 2013, Iran announced the launch of a service called the "Electronic Trust Mark," the term they chose for their national SSL security certificate. The Electronic Trust Mark is issued by the Industries Ministry's Center for eCommerce Development, which gives its stamp of approval to Internet-based communication and transactions.[49] After registering with this Center, which is the website of the Electronic Trust Mark, users must go to **www.mocca.ir**, the website of the Ministry of Industry and Mines, to receive their SSL certificate.

While it is unclear why this particular Ministry was chosen to handle the issuing of Iran's national SSL certificates, what is important is that it is a government ministry: SSL certificates can be thought of as a lock, and anyone possessing a key can unlock the lock (in other words, break the encryption). The government of Iran, through its issuance and distribution of these certificates, has the key to open—and access—any account that uses the national SSL certificates. The stamp of approval then, which appears to guarantee encryption and security to users, actually just ensures government access to the account.



نمایش‌دهندهٔ گواهی:"www.enamad.ir"

این گواهی اعتبارسنجی شده و استفاده از آن برای مقاصد زیر تأیید می‌شود:

گواهی کارگزار SSL

صادر شده برای	
نام معمول (CN)	www.enamad.ir
سازمان (O)	Governmental
واحد سازمانی (OU)	Non-Individual Level 2 (Silver)
شمارهٔ سریال	2C:16:7A:93:00:00:00:00:00:25
صادر شده توسط	
نام معمول (CN)	GICA SSL-Silver(L2)
سازمان (O)	I.R. Government
واحد سازمانی (OU)	Ministry of Industry Mine and Trade
اعتبار	
تاریخ صدور	9/8/2013
تاریخ انقضا	9/8/2014
اثر انگشت	
اثر انگشت SHA1	B3:75:C5:F4:3F:DB:B3:8E:5F:8D:CE:C7:B8:47:33:65:78:B7:27:75
اثر انگشت MD5	9F:D1:9E:A0:0E:57:42:1C:0B:60:4B:97:DC:69:BF:2D

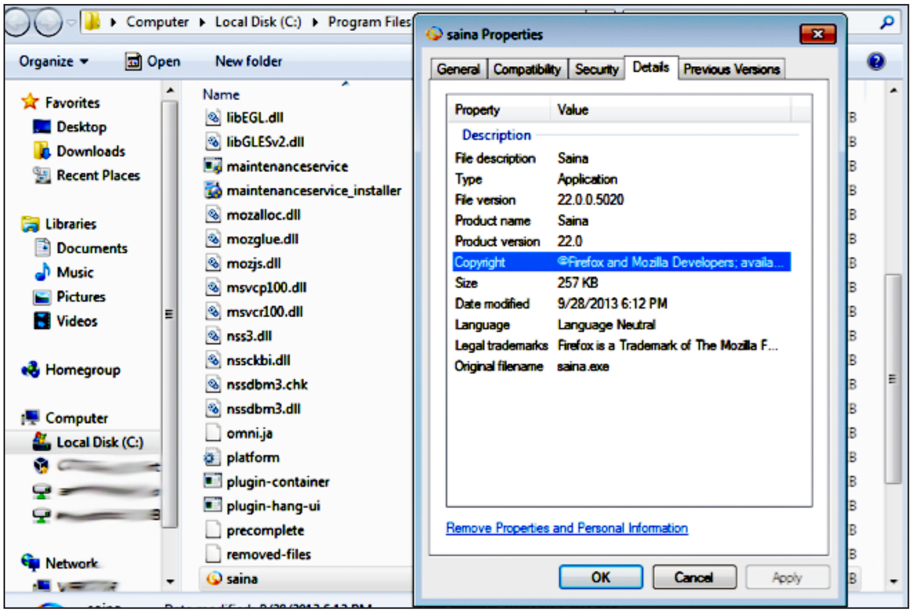
Screen shot of Information Window of the SSL certificates issued by the government, showing their state affiliation.

□ THE NATIONAL BROWSER

The Iranian government has employed two means to ensure the widespread use of its national SSL security certificates (and thus achieve their root certification). One is through the Iranian web browser, Saina, which is provided by state agencies and into which the authorities have built the national SSL certificates.

Saina is central to the success of the government-issued SSL certificates (and thus the government's ability to gain access to content flowing across its National Internet) because Saina uses the SSL certificates issued by the Iranian government. Indeed, Iran's national SSL certificates are valid on no other browser and thus their integration into Saina is critical to their use.

Thus if an individual uses, for example, FireFox, Safari, Google Chrome or Microsoft IE to access Iran's national SSL certificate provider site, **https://www.enamad.ir**, he or she will receive a message warning them that they are using an invalid, or "untrusted" SSL security certificate. If the individual opens the same site with Iran's national browser, Saina, however, he or she will get no warning message.



Property	Value
Description	
File description	Saina
Type	Application
File version	22.0.0.5020
Product name	Saina
Product version	22.0
Copyright	©Firefox and Mozilla Developers; availa...
Size	257 KB
Date modified	9/28/2013 6:12 PM
Language	Language Neutral
Legal trademarks	Firefox is a Trademark of The Mozilla F...
Original filename	saina.exe

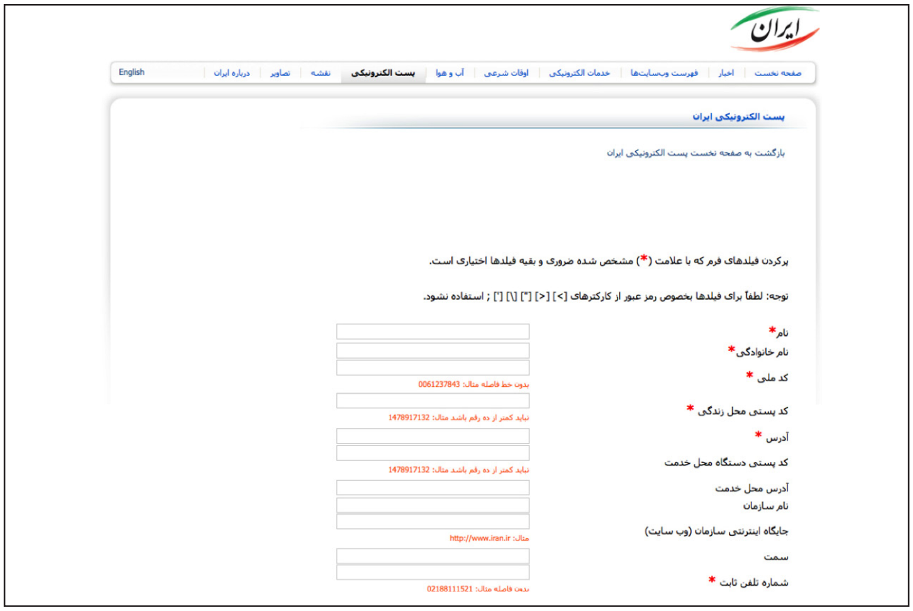
Screen shot of Information Window for Iran's national browser, showing it is based on Firefox.

As more and more people use Iran's Saina browser—and the state-issued SSL certificates contained therein—the national certificates become recognized as trusted, due to their increased usage. This process is particularly insidious, because at a certain point, root certification is achieved and computers will no longer show an error message when using these certificates. The national SSL certificates will thus allow the Iranian government to have access to the online activities of users without their knowledge.

Hamid Reza Hadipour, the deputy manager of the Center for eCommerce Development in charge of the Electronic Trust Mark program, has said that more than 25,000 certificates were issued in 2011.[50] Since then, the number of these certificates has reached 100,000.

In an interview with itanalyze.com, Hadipour also predicted that "with the installment of new systems and increased distribution of [the national SSL] certificates, the goal of issuing 500,000 certificates would be reached in 2014."[51] That is a small number compared to the millions of non-governmental certificates currently used by Iranians online, but it is increasing at a rapid rate.

The ability of the authorities to access account content can have catastrophic consequences.[52] Online content retrieved by the authorities has frequently been used as the sole "evidence" to convict individuals of national security-related crimes and sentence them to lengthy prison terms. In a judicial system routinely marked by denial of due process and the lack of fair trial standards, and in the absence of legal protections or regulations to keep the security agencies in check, the government's ability to access accounts thus poses grave security risks to users.



پست الکترونیکی ایران

بازگشت به صفحه نخست پست الکترونیکی ایران

پرکردن فیلدهای فرم که با علامت (*) مشخص شده ضروری و بقیه فیلدها اختیاری است.

توجه: لطفاً برای فیلدها بخصوص رمز عبور از کارکترهای [<] [>] ["] [\] ['] ; استفاده نشود.

نام*
نام خانوادگی*
کد ملی *
بدون خط فاصله مثال: 0061237843
کد پستی محل زندگی *
نباید کمتر از ده رقم باشد مثال: 1478917132
آدرس *
کد پستی دستگاه محل خدمت
نباید کمتر از ده رقم باشد مثال: 1478917132
آدرس محل خدمت
نام سازمان
جایگاه اینترنتی سازمان (وب سایت)
مثال: http://www.iran.ir
سمت
شماره تلفن ثابت *
بدون فاصله مثال: 02188111521

Registration screen of one of Iran's national email services, showing that registrants must enter their national ID number, address, and phone number, effectively identifying themselves to the authorities.

THE NATIONAL OPERATING SYSTEM

The other means employed by the Iranian government to spread the use of its SSL security certificates is through the national operating system, "Zamin" (or Earth). Zamin was jointly developed by the Information Technology Organization and the Iran Telecom Research Center and released as an open source platform in November 2012.[53] As with the national browser, the authorities have built the SSL security certificates into the national operating system, and Zamin will not recognize Iran's SSL certificates as invalid.[54]

Work on Zamin has been underway for a number of years. The group that designed and documented Iran's national operating system, the National Strategic Headquarters for Open Source Systems, was originally set up at the Office of Technological Cooperation in the presidential palace during Ahmadinejad's administration. On April 28, 2010, Hamid Reza Rabiee, an adviser at the national operating system development project, said that the documentation for Zamin was in the final stages of preparation and had been approved by the Cabinet, clearing the way for its legal institutionalization and for the changeover of government computers from Windows to the national operating system.

The first phase of the launch of Zamin was completed with the development, in November 2012, of the desktop version of the Zamin operating system, which was based on the open source operating system Linux. On November 8, 2012, the Iran Telecom Research Center announced that data centers for the Zamin operating system would be established at Iranian universities.

Iranian officials had promised to launch the second phase of the Zamin system with cloud data processing compatibility and an operating system for hand-held devices by April 2013, but implementation has been behind schedule.[55] Meanwhile, the use of the Windows operating system was banned in government offices on September 9, 2013. The state broadcasting news agency reported that the government directive required the change from Windows to Linux to be implemented within six months.[56] However, while there has been no information on implementation of the directive, it would be technically impossible to carry it out within such a short time frame.

Delays notwithstanding, government efforts on Zamin have been continuing steadily, and the full implementation of such a state-controlled system, in the absence of a legal framework to protect individual privacy, will mean that Internet users in Iran will be effectively sharing their information with the country's security, intelligence, and judicial agencies.

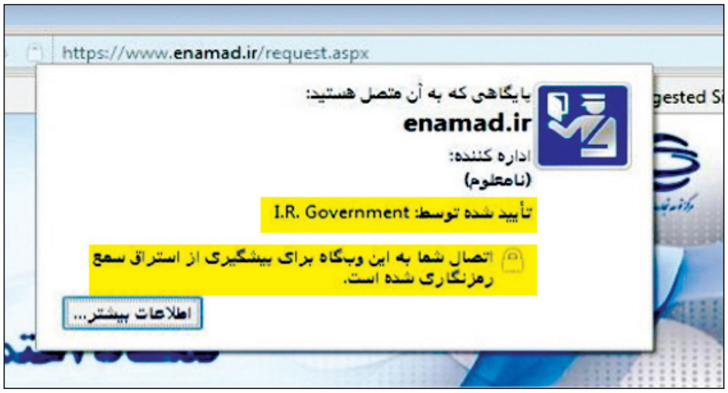
□ NATIONAL SEARCH ENGINES AND SOCIAL NETWORKS

As part of the National Internet, the Iranian government has also developed services such as a national search engine and national social networks, which are designed and implemented largely by the Ministry of Telecommunication's Information Technology Company. Hadi Malek, research director at the Information Technology Company, first announced the creation of the national search engine, "Ya Hagh" (Oh Truth/Holy Truth), on August 28, 2010, as a replacement for Yahoo.[57] Independent analysts believe this search engine has been singularly unsuccessful in attracting Iranian users, and indeed has become fodder for jokes inside Iran. Other search engines have also been developed since then, but none have proved able to attract significant numbers of users. Similarly, national social networks created by the government and designed to appear very similar to Facebook, such as Face Nama[58] and Face Koob[59], have also proved notably unsuccessful in attracting users, as has the Iranian version of YouTube, **www.youtube.ir**.

□ NATIONAL EMAIL

Developing national email providers has also been a component of government efforts to control and access online content and activities. In 2012, Reza Taghipour, Minister of Telecommunication in the Ahmadinejad administration, wrote letters to his deputy and the Central Bank of Iran insisting on the use of domestic email services.[60] He noted that Article 46 regarding informational security objectives in the law concerning the five-year development plan called for banks and communication operators to stop using email services such as Yahoo, Gmail, and Outlook and to instead use nationally-hosted email programs listed by Iran's Internet National Development Management Center.

This Center issued a list of agencies that offered (national) email services, and all government offices were required to use such email services, for example those ending with "iran.ir," "post.ir," and ".chmail." Moreover, in order to register for the email services, users were required to give their National ID number (similar to, for example, a social security number in the United States), their address, and their phone number.



https://www.enamad.ir/request.aspx

پایگاهی که به آن متصل هستید:
enamad.ir
اداره کننده:
(نامعلوم)
تأیید شده توسط: I.R. Government
اتصال شما به این وبگاه برای پیشگیری از استراق سمع
رمزنگاری شده است.

Screen shot showing that Iran’s national browser will not show a warning message (indicating an untrusted certificate is being used) when Iran’s national SSL certificates are used on it.

The implications of this were not lost on the citizenry of Iran, and largely explain the failure of this initiative, which, unlike the national SSL certificates, was relatively easy to discern. Government control over all aspects of the national email service, including, critically, storage of all account information on government servers inside the country (which the government has full access to), means that the government has full access to the account—the authorities can read the body of the email, access any attachments, and see any contacts. In addition, these national email services are not securely encrypted. While some of them do not use valid international SSL security certificates, others do not use any SSL certificate at all. As a result these accounts are completely open—not only to the government but to hackers as well. Moreover, the requirement that users of these national email services provide their national ID number (as well as address and phone number) means that all anonymity is gone. Once a user provides this information, they have effectively identified themselves to the government. For those engaged in political or social activism, state access to their email content would have catastrophic consequences given the government’s record of imprisoning those who engage in online activism.

To date, the government has been notably unsuccessful in this aspect of the National Network. For example, when the government required banks to open accounts only for individuals who listed a national email account, the banks found that individuals simply refused to open accounts at those institutions. The banks subsequently dropped the requirement of a national email account.

□ NATIONAL VIRTUAL PRIVATE NETWORKS (VPNs)

One of the principal ways that Iranians have been able to maintain access to the global Internet has been through the use of Virtual Private Networks (VPNs), which allow users to circumvent government filters by providing encrypted links to networks based abroad, effectively enabling a computer to function as if it is based in another country. The computer is thus able to directly connect to the global Internet. As a result, the authorities have increasingly moved to target this access, by shutting down VPN ports and simultaneously offering and encouraging the use of “legal VPNs” that are provided by a government organization (the Telecommunication Infrastructure Company, affiliated to the Telecommunications Ministry).

Government shut downs of VPNs have tended to come in waves. For example, VPNs were shut down during the 2009 post-presidential election crackdown, again in October 2011 by the state filtering Working Group because they were "allowing access to criminal content," and again in May 2013. Yet users have usually been able to eventually reestablish VPN ports, sometimes, in fact, quite quickly. The government thus sought a more effective way of countering these (non-government) VPNs.

Its answer was national (or "legal") VPNs, provided by the government. National VPNs were first mentioned by the head of the Passive Defense Organization, which is under the Ministry of the Interior, in October of 2012. On January 27, 2013, Mehdi Akhavan Behabadi, the director of the Supreme Cyberspace Council, announced the establishment of the legal VPNs in an interview with the Mehr news agency, and on February 19, 2013, the national VPN service was launched.[61] The national VPNs are issued to individuals through the website **www.vpn.ir**, a portal that cannot be accessed from abroad.

Similar to the government's national email service, however, its VPN initiative has met with little success; there has been scant interest in using government-issued VPNs where filtered sites remain filtered, since the purpose of using VPNs is to access filtered sites. Indeed, after the election of President Rouhani in June 2013, Mahmoud Khosravi, the head of the Telecommunications Infrastructure Company said the national VPN project had in fact failed.[62] He added that despite all efforts to inform the public and the expenditure of millions of dollars, only 26 companies had registered for national VPNs.

Nevertheless, hardliners in the government have not ceased their attempts to counter the use of (non-government-issued) VPNs. On May 12, 2014, the FATA cyber police force declared that VPNs were allowing criminal activity and the Judiciary Commission of the Majlis (the Iranian Parliament) began discussion of a bill to punish those who use it. If made into law, it could significantly reduce the number of VPN users — and with it, access to the global Internet for Iranians.[63]

In sum, progress on the development and implementation of Iran's National Internet and all its various components has been made—even if unevenly and behind schedule—and it is continuing. Reza Bagheri-Asl, the acting deputy head of the government's Information Technology Organization, announced on April 21, 2014, that the National Internet had become fully operational for government offices.[64] He specifically cited the cooperation of the Telecommunications Ministry, the Information Technology Organization, and the Telecommunication Infrastructure Company, as well as telecommunication operators. Independent analysts have questioned whether implementation has actually been fully achieved, but the statement indicates progress is underway.

□ THE NATIONAL INTERNET AND DOMESTIC POLITICS IN IRAN

Officials in Iran have attributed the delays and uneven progress in the development and implementation of the country's National Internet to technological problems, difficulties created by international sanctions against the country, and budgetary constraints. Yet these delays must also be seen within the context of the political infighting that has accompanied the project.

Image of the desktop of Zamin, Iran's national operating system.

Hardliners, ensconced in the security, intelligence, and judicial services, and dominant in the Iranian Parliament, view Internet freedom as tantamount to opening the gates to the enemy, and are pushing hard for full implementation of the National Network. The Rouhani administration, however, is more ambivalent about its support for the National Network. It views Internet freedom as part and parcel of the economic revitalization and modernization of the country, which is the central priority of the administration. Thus while the Rouhani administration is amenable to creating the National Network, and has in fact supported its continued implementation, it has also signaled that it doesn't wish to preclude access to the global Internet.

Indeed, the Rouhani Administration has several times explicitly denied any intention to prevent Iranians' access to the global Internet. President Rouhani's Telecommunications Minister Mahmoud Vaezi assured opponents of the National Information Network that its launch would not result in a cut off from the global Internet. "I assure you that this will never happen," he said and added that the National Network would become operational in 2015, increasing the capacity of the Internet from 70 GBs per second to 700 GBs per second.[65] In addition, a number of ministers in Rouhani's administration are openly active on social networks such as Facebook and Twitter, sending a strong signal that activities on these international social networks are acceptable.

This political infighting has played out in the budgeting allotted to the Network. Nasrollah Jahangard, the secretary of the Supreme Technology Council and Deputy Minister of Telecommunications, said in a speech at the Society and Cyberspace Conference in Iran in February 2014 that in order to implement the remaining commitments of the National Information Network over the next four years, as detailed in the five-year development plan, $50 billion in investments was needed—but that the government had so far allocated only $17 billion in state funds for it.[66]

The Rouhani administration has argued that the government does not have any more funds available in the budget to allocate to the project. Yet hardliners in Parliament continue to push for more funding, arguing that it is national priority, a position in accordance with their view that open Internet access is a threat to national security.

Recent statements made by officials in the Rouhani Administration appear to signal a slight shift in their strategy regarding the National Internet. While hardliners have kept to their vision of the National Internet as a wall encircling the country, preventing any access to the global Internet, the administration now seems to envision a National Internet in which walls around the country are present—but with (government-controlled) gates to allow communications with the international community through the global Internet, albeit under tight security controls embedded in the network to monitor users.

Iranian officials do not shy away from admitting that the National Network will enable government agencies to monitor the activities of online users. Ali Hakim-Javadi, the former head of the Information Technology Organization in charge of implementing the National Information Network, and the current head of the Fourth Telecom Operator (IranianNetCompany), said in an interview on February 19, 2014, “There are certain mindsets especially among the young generation who fear they will be monitored if they use National Internet services. But the fact is that all Internet users everywhere are monitored.”[67]

Asked if he did not think monitoring users would be a breach of individual privacy, Hakim-Javadi said, “Be sure that even at present all the activities of users online are being watched but they aren’t aware of it. But there are legal issues involved in monitoring. One of the issues we have in our country regarding cyberspace is that we have few laws. Therefore we must define the legal frameworks and do some cultural work to let people know that they are being watched. We have no technical problems as far as surveillance is concerned.”[68]

Security Agencies and the Prosecution of Online Activists

In addition to the Iranian state's efforts to develop the technological infrastructure of Internet control, the Judiciary and security organizations have also pursued the identification and prosecution of online activists. This is done through a variety of organizations, some of them official, some semi-official, and some that are almost completely opaque, facilitating a near complete lack of accountability.

FATA, THE IRANIAN CYBER POLICE

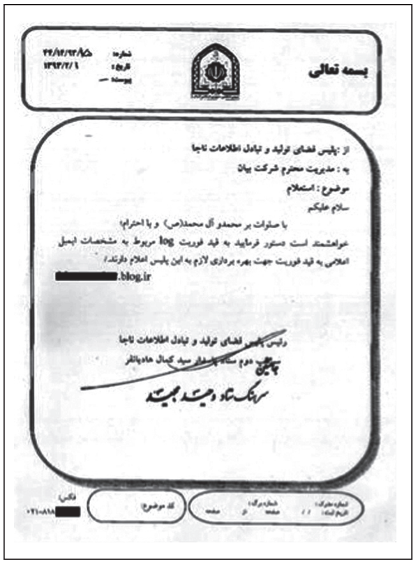
On January 23, 2011, the Iranian national police force established the Cyber Police, also known as FATA, as the cybercrime unit of the national police force.[69]

In addition to fighting cybercrime, the officials justified the formation of the force as necessary to fight terrorism, and to guard against alleged threats to national security. However, FATA's activities also include monitoring the activities of civil and political activists. During the ceremony establishing FATA, Chief of Police General Esmail Ahmadi Moghaddam said, in an explicit reference to the role of online social networks in the protests following the disputed 2009 presidential election, "Social networks on the Internet brought a lot of harm to our country because of spreading rumors and allowing anti-state groups to help each other."

In essence, FATA pursues, through harassment, arrest, and interrogation, any citizen who expresses dissenting views online. Indeed, FATA officials have publicly boasted that they monitor all Internet activity around the clock. FATA's arrest of Sattar Beheshti, the 35-year-old blogger who died under torture while in FATA's custody in November 2012, only a few days after his October 31, 2012, arrest, is indicative of their aggressive pursuit of online activists.[70]

FATA pursues, through harassment, arrest, and interrogation, any citizen who expresses dissenting views online.

The FATA cyber police have also pressured Internet providers to provide them with evidence they can use to pursue online activists. One Tehran-based company, Bayan, publicized FATA's attempts to illegally obtain personal information about one of its online customers, publishing copies of four letters exchanged with FATA, including one in April 2014 in which FATA demanded that the company immediately hand over the



بسمه تعالی

شماره: ۳۲/۱۲/۹۳/۸۵
تاریخ: ۱۳۹۳/۲/۱
پیوست: —

از : پلیس فضای تولید و تبادل اطلاعات ناجا
به : مدیریت محترم شرکت بیان
موضوع : استعلام
سلام علیکم

با صلوات بر محمدو آل محمد(ص) و با احترام؛
خواهشمند است دستور فرمایید به قید فوریت log مربوط به مشخصات ایمیل اعلامی به قید فوریت جهت بهره برداری لازم به این پلیس اعلام دارند./

[redacted].blog.ir

رئیس پلیس فضای تولید و تبادل اطلاعات ناجا
سرتیپ دوم ستاد پاسدار سید کمال هادیانفر
جانشین
سرهنگ ستاد وحید مجید

شماره مجوز: / تاریخ ثبت: / /
شماره برگ: صفحه از صفحه
کد موضوع:
فکس: ۰۲۱-۸۸[redacted]

Image of FATA cyber police’s letter to the Bayan company, pressuring them to reveal customer information.

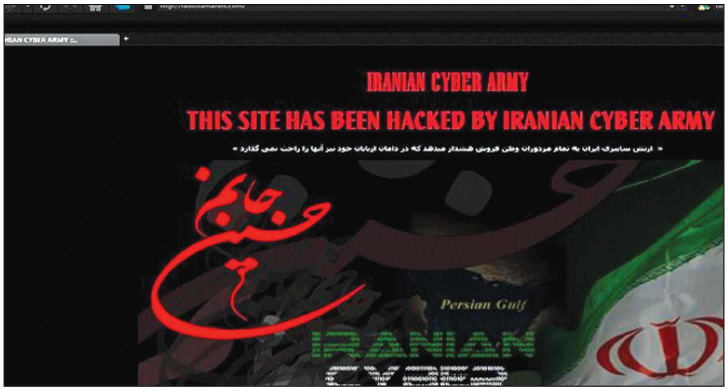
activity records of a user for “necessary action.” Bayan resisted FATA’s demands and wrote to its customers on May 7, 2014: “Carrying out our mission in protecting the privacy of our customers requires technical and legal expertise. Therefore one of the difficult, time-consuming and expensive aspects of our company is the legal department whose activities are largely unknown to our customers. The following is an example of these efforts to protect the rights of our customers.”

□ CYBER ARMY

As its name signifies, Iran’s Cyber Army is the offensive arm of the state’s cyberspace activities, charged with attacking and bringing down any domestic website that engages in activities the authorities perceive as transgressive—as well as hacking and disrupting the websites of perceived foreign enemies.

Iran’s Cyber Army was created by the Revolutionary Guard Corp (IRGC) in the wake of the 2009 protests that followed the disputed presidential election in Iran that year. The protestors heavily utilized online platforms to mobilize and organize their protests, and as such the Guards sought to control all online channels of communication, especially social networks, in order to prevent the protestors from utilizing them. They began their activities by posting pictures of the protesters (so that they could be targeted for harassment and turned in to the authorities) and hacking Green Movement (the reformist political movement that arose in the wake of that election) and other opposition websites.

In early March 2010, Gholamreza Jalali, the head of the Ministry of the Interior’s Passive Defense Organization, announced that the “Cyber Warfare Headquarters of the Islamic Republic” would be established soon and invited the cooperation of “good intentioned” hackers.[71] In an interview with the Mehr news agency on March 13, 2010, General Ali Fazli, the Commander of the Revolutionary Guards, formally confirmed the existence of



IRANIAN CYBER ARMY

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

« ارتش سایبری ایران به تمام مزدوران وطن فروش هشدار میدهد که در دامان اربابان خود نیز آنها را راحت نمی گذارد »

Screen shot of Radio Zamaneh's home page showing it has been hacked by Iran's Cyber Army.

the Cyber Army within the Guards and said it consisted of "experts from among Basiji academics, university students, religious seminary students, and Basiji sisters (female Basiji militia members)."[72] Ebrahim Jabbari, commander of the Ali Ibn-e Abitaleb division of the Guards in Qom told Fars news agency on May 21, 2010, that not only had the Guards formed the Cyber Army but that it was "second in the world."[73] And in December 2011, Mojtaba Zolnour, the deputy commander of the Guards at the time told the weekly Noh-e-Day that while Iran was new in the field of cyber war, the use of the Cyber Army had resulted in successes in "hacking, disabling, and filtering enemy sites."[74]

The Iranian Cyber Army has taken specific responsibility for hacking websites such as Radio Zamaneh, the Green Wave of Freedom, Twitter, China's Baidu search engine, Amir Kabr University newsletter, and Jaras, an opposition news site.[75] In addition to bringing down websites it disapproves of, the Cyber Army also produces malicious botnet programs, which attack a targeted site by marshaling broad attacks involving many (unsuspecting) computers in the attack. According to a report in zdnet.com, one Cyber Army botnet attack infected some 20 million computers through the Windows operating system.[76]

While the Cyber Army is a unit of the Revolutionary Guards, its actual structure and makeup are opaque and its lines of authority blurred. Its shadowy nature facilitates the lack of accountability it enjoys as it carries out its mission, namely the extension of state repression into cyberspace. Indeed, the effective anonymity of the Cyber Army is critical to its central role—to monitor, hack, and bring down websites that are perceived as posing a potential challenge to the authority of the government—and its ability to function extra-judicially, carrying out disabling attacks on websites and removing these voices of dissent, without court order or any responsible official that a citizen or organization can question or hold accountable.

All of the various organizations typically work together. For example, material that is obtained by a hacking operation is then used in the arrest and interrogation (and, frequently, torture) of targeted individuals by police, intelligence, and security officials, and then the illegally obtained online content, as well as the forced confession elicited under torture or threat during interrogation, is then used to convict the individual in court under typically vague national security-related charges.

□ SECURITY ACTIONS BY OTHER ORGANIZATIONS

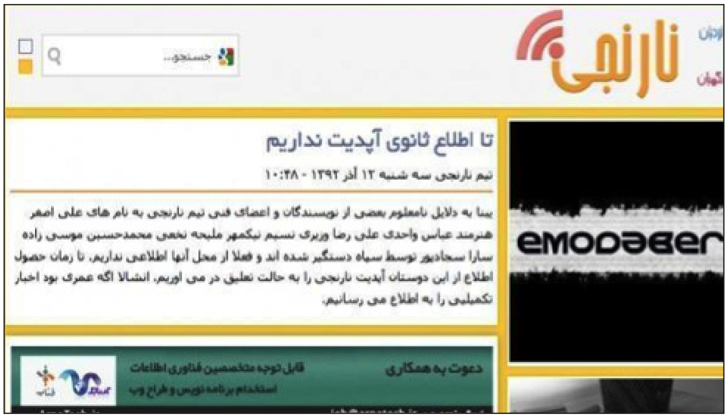
Other state organizations, official and semi-official, are active in the persecution of online activists as well. In fact, arrests of such individuals have increased since Rouhani's August 2013 inauguration, reflecting intensified efforts in this area by hardliners in the security and intelligence services.

For example, on December 3, 2013, the Narenji website posted a note on its site that members from its technical and writing teams had been arrested by units of the Islamic Revolutionary Guards. The arrested included Ali Asghar Honarmand, Abbas Vahedi, Alireza Vaziri, Nasim Nikmehr, Maliheh Nakhaie, Mohammad Hossein Mousazadeh, and Sara Sajadpour. The Narenji website was active in reviewing new information technology tools. In 2010, it received the award for Best Information at the Third Iranian Websites Festival and in 2013 Germany's Deutsche Welle Persian radio service named Narenji the Best Persian Blog. On June 19, 2014, Yadollah Movahed, the public prosecutor of Kerman, said that eleven cyber activists in the city had been tried and condemned to between one and eleven years in prison (seven of which had been arrested in October 2013). Movahed did not reveal their names but said they were in connection with the Pot Shargh Guashir case, which is Narenji's parent company.[77]

> ***The effective anonymity of the Cyber Army is critical to its central role—to monitor, hack, and bring down websites that are perceived as posing a potential challenge to the authority of the government—and its ability to function extra-judicially without court order or any responsible official that a citizen or organization can question or hold accountable.***

In addition to the arrest of the Narenji members, the public relations office of the Revolutionary Guards in Kerman announced on December 22, 2013, that the Guard's intelligence unit in Kerman Province had hacked nine "anti-Islamic sites" in an extensive cyber operation, including Neday-e Sabz-e Azadi, Sabznameh, Norooz, Ostanban, 30mail, Nogam, Iran Opinion, and Degarvajeh. "The anti-Islamic sites, which had been set up with millions [of dollars] in financial backing and support from internal seditious elements, were completely blocked from access," Fars news agency quoted in its report.[78]

Revolutionary Guard agents also arrested the online activist Moslem Boushehrian on January 22, 2014, according to the Jaras website, as he entered Tehran's international airport.[79] Boushehrian had been studying in China in recent months and was active on social networks. He was reportedly taken to an unknown location and, as of this writing, his family has still not been able to locate him, despite numerous visits to judicial centers seeking his whereabouts, or learn of any charges that have been filed against him. On January 25, 2014, three social network activists, Sasan Jannatian, Siavash Jannatian, and Reza Alenasser were arrested in Mashhad.[80] News reports indicate that as they were leaving Azad University dormitory they were picked up by several armed agents with walkie-talkies and were forced into two cars. Siavash Jannatian was


نارنجی
جستجو...
emodaber
دعوت به همکاری
قابل توجه متخصصین فناوری اطلاعات
استخدام برنامه نویس و طراح وب

تا اطلاع ثانوی آپدیت نداریم

تیم نارنجی سه شنبه ۱۲ آذر ۱۳۹۲ - ۱۰:۴۸

بنا به دلایل نامعلوم بعضی از نویسندگان و اعضای فنی تیم نارنجی به نام های علی اصغر
هنرمند عباس واحدی علی رضا وریری نسیم نیکمهر ملیحه نخعی محمدحسین موسی زاده
سارا سجادپور توسط سپاه دستگیر شده اند و فعلا از محل آنها اطلاعی نداریم. تا زمان حصول
اطلاع از این دوستان آپدیت نارنجی را به حالت تعلیق در می اوریم. انشالا اگه عمری بود اخبار
تکمیلی را به اطلاع می رسانیم.

Image from the Narenji website posting news regarding the arrest of its members.

a student at Mashhad's Azad University and had an active student blog. Sasan Jannatian had previously been detained as a student activist during the 2009 protests. Reza Alenasser had also been previously summoned and warned by security agencies in Khuzestan Province regarding his blog, "Kankash" (Inquiry).

Judicial officials have done their part to ensure hefty sentences to those convicted of transgressions online—at times to an extent greater than that allowed under Iranian law. In July 2014, for example, eight young Iranians were sentenced for their activities on Facebook by Branch 28 of the Tehran Revolutionary Court under Judge Moghisseh to prison sentences that were up to three times longer than permissible under Iran's own laws.[81]

The official news agency, Islamic Republic News Agency (IRNA) reported on July 13, 2014, that the individuals were convicted on charges of "assembly and collusion against national security," "propaganda against the state," and "blasphemy, insulting Heads of Branches, and insulting individuals."[82] If the case had been handled according to the law, even at maximum sentence, none of them should have received more than 7.5 years in prison. According to Article 134 of the New Islamic Penal Code, which was implemented in May 2014, if a suspect faces three or more charges, the judge must only rule for the maximum punishment of one of those charges. However, they received, in order of descending severity, 21 years, 20 years, 19 years and 91 days, 18 years and 91 days, 16 years, 14 years, 11 years, and 8 years in prison. All charges that were brought against these individuals were based on content and photographs they had posted on their Facebook pages. The IRNA report indicated that it was units from the Revolutionary Guard's Sarallah Base that had arrested them.

These few examples are representative, not comprehensive. Yet they demonstrate that multiple official and semi-official organizations, including those whose remit does not specifically pertain to Internet issues, pursue online activists and IT professionals who disseminate technological information online. Indeed, this pursuit has not only has continued, it has intensified.

Seeking International Technology Firms’ Compliance

In spite of all the authorities’ efforts to censor the Internet and punish those who seek to use it for social or political activism, the government has yet to achieve full control over the Internet and its use. Recognizing that Iran’s National Internet and all of its various components are far from complete, and that many Iranians in fact still extensively use Internet services provided by private international technology firms that are not under the control of the Iranian state, the authorities have mounted a parallel effort to build relationships with such firms. The authorities hope to obtain these firms’ compliance with the government’s Internet policies for services used inside Iran.

Iran represents a large potential market for such firms: its population is young and 77 million strong and its Internet penetration is significant and growing steadily. A physical presence inside the country would open up sales of software and services that are currently impossible for these firms. For Iran, the benefit would be the ability to promote terms and a working relationship that would require these firms to comply with their Internet policies in such areas as filtering sites or limitations on content. Moreover, if the company is physically inside the country, the authorities are keenly aware that it would be easier to develop a close working relationship in which they can request information about users or account activities—and these requests would be made to companies that would have a great deal of detailed information about their Iranian users.

Google has warned Iranian Gmail users about concerted state-backed cyber attacks at least twice this year.

Mahmoud Khosravi, the head of the Telecommunication Infrastructure Company, said on December 26, 2013, that the Islamic Guidance Ministry and the Information Technology Organization had started negotiations with major Internet companies, including Google, in order to bring them to Iran and convince them to accept and comply with Iran’s Internet policies. Google has so far declined to give an official public response to Iran’s request. If such an agreement were to be reached, the Iranian government would likely seek to extend this to agreements with other international firms.

In the case of Google, at least, it does not seem that the company is naïve or ignorant of the Iranian authorities’ activities vis-à-vis the Internet. Google has warned Iranian Gmail users about concerted state-backed cyber attacks at least twice this year. Google stated that the warnings were based on reports received from users about attacks on their accounts, which were carried out by state (and not civilian) hackers.

The Rouhani Administration and Internet Freedom

While Hassan Rouhani campaigned for the presidency in Iran on a platform explicitly promoting Internet freedom, one year into his presidency there has been little progress to date on this front. In fact, as this report has shown, development of Iran's National Internet continues, the filtering of mobile applications has increased, and the persecution of online activists and information technology professionals has intensified.

Rouhani's policies have so far demonstrated that he is focused on pushing through his foreign policy objectives (namely, the P5+1 nuclear negotiations) and has thus been disinclined to simultaneously use his limited stock of political capital on domestic issues. Yet Rouhani has been more vocal on the issue of Internet freedom, even if his rhetoric has not translated into concrete policies, than he has on other domestic issues, in large part because Internet access (similar to the nuclear negotiations that will end the country's international isolation) is integral to his overriding policy objective—the economic revitalization and modernization of the country.

Rouhani has been more vocal on the issue of Internet freedom, even if his rhetoric has not translated into concrete policies, than he has on other domestic issues.

Asked about Internet access in an interview with NBC on September 19, 2013, Rouhani said: "The government's view is that the people should have access to all the information in the world."[83] Rouhani has also defended people's access to social networks as a necessity. In the same interview, he said: "Networks have an important role. During my election campaign, I did not have a strong team but all my supporters, especially the youth, used these social networks. They still use them and in fact monitor the government's work. I am happy that young people are so active and even check on the government's actions."[84]

Other officials in his administration have also spoken in favor of people's access to social networks. Minister of Islamic Guidance Ali Jannati told Fars news agency on November 15, 2013, "Facebook is a social network. I do not consider it a crime to use it. People have healthy and proper communications there. I myself have a presence in Facebook."[85] In May 2014, Telecommunications Minister Mahmoud Vaezi said "Only 15 percent of Facebook's content consisted of unsuitable material and photos and the rest is beneficial and can easily be used and managed inside the country."[86] Indeed, in a tacit stamp of approval for these social networks, a number of senior government officials, including not only Rouhani but his foreign minister Javad Zarif and others as well, have joined the millions of Iranians who have active pages in their name on social networks such as Facebook and Twitter, even though the sites are officially blocked inside the country.

Moreover, Rouhani has, upon occasion, taken specific actions to advance Internet freedom. His order to unblock the mobile application WhatsApp, after the Working Committee had blocked it, was a rare instance of administration pushback against the hardliners. Yet while this case has been frequently cited as an indication that he wishes to advance Internet freedom in the country, it also revealed that Rouhani can—when he desires—wield his not insignificant powers to push back against hardliners' efforts at increased censorship. This raises a fundamental question: namely, why Rouhani has not done more to promote Internet access?

To be sure, many argue that Rouhani has limited powers to address these issues. Khamenei and the various committees he has established to oversee the Internet, such as the Supreme Council and the Working Group, are dominated by hardliners who share Khamenei's view of the Internet as an inherently hostile force. Administration members are a permanent minority on both bodies.

Rouhani's order to unblock the mobile application WhatsApp, after the Working Committee had blocked it, was a rare instance of administration pushback against the hardliners.

Moreover, Rouhani has faced withering criticism by hardliners for his statements supporting Internet freedom, for the presence of administration officials on social networks such as Facebook and Twitter and for their support of people's access to it, and for the few actions he has taken to defend Internet access, such as the unblocking of WhatsApp. In a typical remark, the conservative leader of Friday Prayers for the city of Mashhad, Ayatollah Ahmad Alamolhoda, stated, "The Young Journalists Club has quoted the government's Telecommunications Minister that the government should remove filters and unblock Facebook….That means we should open our gates to the enemies of Prophet Mohammad. Breaking the block on Facebook would bring nothing other than insults against the Prophet and his family. Our youth will be flooded with anti-religious material. Is this how you want to conduct cultural resistance?" Alamolhoda added, "Have the people voted for this government, this president and this Majlis [Parliament] to break the filter on Facebook? You say only 15 percent of Facebook is useable [sic]. Is that enough to break the filter and open the gate [to] the enemies of God?"[87]

After months of pressure from hardliners to maintain blocks on various social networking sites and applications, Guidance Minister Ali Jannati pushed back, albeit gently, telling the Mehr news agency in July 2014, "The dispute today is over the details. One group believes that Viber should be filtered. Another group is against it. These differences also exist among the members of the Working Group to Determine Instances of Criminal Content on the Internet. But we should not act according to personal tastes. We should act according to the law."[88]

Defending the government's hitherto inability to remove the block on Facebook despite the fact that many officials in the administration actively use the site, Jannati also called attention to the domination of key Committees by hardliners, stating in a meeting with Iranian digital professionals, "The filtering committee [i.e. the Working Group] is in charge of removing filters. It is not under the direct supervision of the [Islamic]

Guidance and Culture Ministry. This [Guidance] ministry only has a representative in the committee. We have to speak with all members of the committee to make it legal to use Facebook and all other social networks."[89]

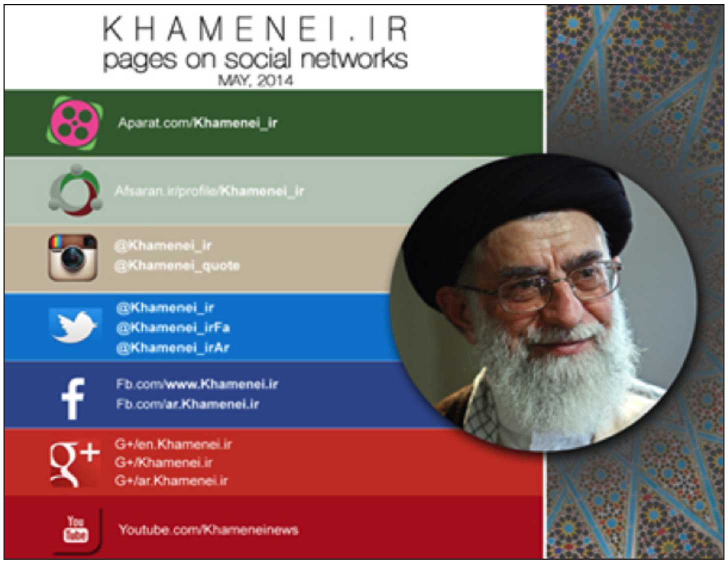
Nevertheless, it is also true that development of Iran's National Internet is being led and implemented by the Ministry of Telecommunications, which is under the direct authority of the executive branch, and that this Ministry's budget is allocated by the Rouhani administration. The Ministry of Culture and Islamic Guidance, which has assumed an increasing role in filtering sites (independent of the Supreme Council and the Working Group), is also under the direct authority of Rouhani, and receives its budget from the administration. In addition, Rouhani chairs the Supreme Cyberspace Council, and has attended its meetings since assuming the presidency, reflecting the importance he gives to Internet issues and the Council's decisions regarding them. Thus Rouhani clearly has avenues of influence, as the WhatsApp incident revealed, and it remains an open question why he has not done more to defend and advance Internet freedom in the country.

Development of Iran's National Internet is being led and implemented by the Ministry of Telecommunications, which is under the direct authority of the executive branch, and this Ministry's budget is allocated by Rouhani.

Given Rouhani's support for the continued implementation of the National Internet, it appears he will most assertively promote Internet access in so far as it advances the economic revitalization of the country—a goal that is central to his administration's agenda. Thus he has consistently pushed for increasing the bandwidth available inside Iran, which is necessary for effective professional, commercial and academic use. On June 6, 2013, he stated, "The current Internet bandwidth [available] is not what the Iranian people deserve…. Today we live in a world of communication. Unfortunately, however, some people think they are living in the 19th century."[90] On May 17, 2014, he publicly expressed dissatisfaction with Iran's 154th global ranking in terms of bandwidth capacity, saying, "The Telecommunications Ministry plans to implement third and fourth generation technologies as soon as possible, bringing broadband not only to homes and businesses, but also for mobile devices."[91]

Rouhani achieved significant progress in increasing bandwidth in September 2014, when the Ministry of Communications opened up licenses to provide 3G and 4G mobile services in the country. Previously, there had been only one mobile provider, RighTel, allowed to provide 3G services. With RighTel's reported 1.5 million customers,[92] this represented a relatively small percentage of the almost 57 million mobile phone users inside Iran as of 2013.[93]

The opening up of 3G and 4G licenses represented a victory against hardliners, who railed against fast Internet speeds (and the access to content such speeds would allow) and had long relied on the practice of slowing down Internet speeds to the point where its use was rendered effectively impossible. In August 2014, Ayatollah Nasser Makarem Shirazi, one of the country's highest clerical authorities, issued a fatwa that stated, "All third generation [3G] and high-speed Internet services, prior to realization of the required conditions for the National Information Network, is against Sharia [and] against moral and human standards." [94]



KHAMENEI.IR
pages on social networks
MAY, 2014

Aparat.com/Khamenei_ir

Afsaran.ir/profile/Khamenei_ir

@Khamenei_ir
@Khamenei_quote

@Khamenei_ir
@Khamenei_irFa
@Khamenei_irAr

Fb.com/www.Khamenei.ir
Fb.com/ar.Khamenei.ir

G+/en.Khamenei.ir
G+/Khamenei.ir
G+/ar.Khamenei.ir

Youtube.com/Khameneinews

A poster on Ayatollah Khamenei's Facebook page promoting his social media accounts. The same social networks are officially blocked for Iranian citizens.

Yet the administration pressed forward and has so far succeeded in this initiative. In a direct rebuttal on September 1, 2014, Rouhani said, “We cannot shut the gates of the world to our young generation…. Once, there was a time that someone would hide his radio at home, if he had one, to use it just for listening to the news. We have passed that era.”[95]

In addition to focusing on upgrading the technological infrastructure, Rouhani has promoted Iran’s international engagement on information technology issues. Iran has resumed high-level participation in the World Summit on the Information Society (after a scant presence during the 2005-2013 Ahmadinejad administration, when there was little interest in an organization where countries make proposals to “establish the foundations for an Information Society for all”), and his administration has facilitated the attendance of Iranian experts, academics, and journalists in the summit. During the last summit, Iran’s Telecommunications Minister invited the secretary general of the International Telecommunication Union to visit Iran. In addition, the Telecommunications Ministry recently issued a tender for “Tadbir 1,” the project to upgrade and expand the country’s Internet infrastructure, and reports suggest that the Rouhani government is trying to bring Western companies into the project.[96]

The Rouhani administration’s willingness to be more engaged with the international community, especially through its participation in UN forums, international organizations, and international information communication technology (ICT) conferences (such as the International Telecommunication Union (ITU), the Internet Corporation for Assigned Names and Numbers (ICANN), the World Summit on the Information Society (WSIS), and the Internet Governance Forum (IGF), presents an opportunity for civil society in Iran to participate professionally and present a credible voice on Internet freedom issues in a multi-stakeholder process. This process will help promote Iranian officials’ accountability regarding their international obligations on UN principles and Internet governance. Civil society must remain vigilant, however, that the Iranian government does not use its participation in these conferences and other forums to obscure its crackdown on cyberspace.

Overall, the Iranian state seems to have a conflicted relationship towards the Internet—embracing it when it advances a desired agenda, controlling it when it challenges that agenda. The quintessential example of this is Khamenei, who promotes anti-Internet policies and yet has accounts in nearly all officially banned social networks, such as Facebook, Twitter and Instagram, in Persian, English, and Arabic. Khamenei, as almost all other Iranian officials, hardliners and moderates alike, recognizes that the Internet has become an indispensable tool for reaching the public. Thus, for example, hardliners cheered on the wave of remarks on Twitter, YouTube, and other social networks by Iranian citizens that ridiculed Israeli Prime Minister Benjamin Netanyahu for his inaccurate remarks about Iranians not being able to wear jeans. Reflecting an increasingly contradictory relationship with social media, expression on such sites is acceptable, but only if the party line is followed.

Rouhani achieved significant progress in increasing bandwidth in September 2014, when the Ministry of Communications opened up licenses to provide 3G and 4G mobile services in the country.

Advocates of Internet freedom, both inside and outside Iran, hope that Rouhani will use all of his authority and powers to promote Iranians' full and safe access to the Internet, in the same way that he has successfully promoted mobile infrastructure upgrades such as increased bandwidth through the provision of 3G and 4G services.

Conclusion

In 2013, Reporters Without Borders named Iran one of the world's five worst enemies of the Internet, along with China, Syria, Bahrain and Vietnam.[97] This report by the International Campaign for Human Rights in Iran has shown that if the Iranian government is able to fully implement the technological initiatives currently underway, the level of Internet control and censorship in the country will further intensify. Most critically, the government's ability to covertly access and monitor online content will significantly increase, posing grave dangers for individuals engaged in any kind of political or social activism. They will likely face arrest, detainment without access to counsel, possible torture, and subsequent conviction after trials lacking any semblance of due process, on vague national security charges that will put them behind bars for years.

Iran's description and justification for its Internet-related projects are profoundly misleading. While bandwidth and other technological advances may well be achieved (albeit from an extremely low starting point), and certain applications blocked or encumbered now due to sanctions may well become more accessible to Iranians, this is neither the central purpose nor the principal outcome of its Internet initiatives. Indeed, these justifications serve only to obscure the main objective. Rather, Iran's National Internet project, its continued filtering activities, and its intensified online monitoring capabilities are aimed at stamping out political or social activism online (or, indeed any independent online expression) and prosecuting those who attempt to engage in it. These projects will allow the government to further control and restrict access to information in Iran, and to monitor all content that flows across the National Internet. These are direct violations of fundamental human rights that are protected by international law[98] and Iran's own constitution.[99] In 2012, the U.N. passed a resolution recognizing the universal right to Internet access and freedom of online expression, and calling on all governments to ensure access to the Internet by all citizens. Until the domestic context in Iran allows this, the international community must make every effort to alert Iranian society to online vulnerabilities, assist them in the development of technologies that will counter such dangers and repression, urge the Rouhani administration to honor its pledges to defend and promote Internet freedom in Iran, and urgently defend in word and deed the universal right to freedom of expression and access to information.

Endnotes

1.**"Fulfilling Promises: A Human Rights Roadmap for Rouhani,"** *International Campaign for Human Rights in Iran,* August 21, 2013. http://www.iranhumanrights.org/2013/08/introduction-rouhani/.

2.**"Supreme Leader Appoints Members of the Supreme Cyberspace Council,"** *Official Website of Ayatollah Khamenei,* March 7, 2012, http://www.leader.ir/langs/fa/index.php?p=contentShow&id=9213.

3.**"Full Text of the Computer Crimes Law,"** *Official Website of the Working Group to Determine Instances of Criminal Content on the Internet,* http://internet.ir/law.html.

4.**"Fifth Five Year Development Plan of the Islamic Republic of Iran (1390-1394),"** *Islamic Parliament Research Center,* http://rc.majlis.ir/fa/law/show/790196.

5.**"40 Billion Tomans Spent on Creation of National Data Centers,"** *Khabaronline,* May 21, 2012,

http://khabaronline.ir/detail/214889/ict/5121.

6.**"Obtaining SSL Security Certificates Made Obligatory,"** *Ministry of I.C.T., Islamic Republic Post Company,* November 24, 2013, http://goo.gl/pbm1D3.

7.**Website of the Iranian Web Browser Siana,** http://saina.matma.ir/.

8.**Website of the Zamin Operating System,** http://xamin.ir/en/

9.**"Government Bans Use of Windows; Linux is Approved,"** *Islamic Republic of Iran News Network,* September 9, 2013, http://goo.gl/b2zTsS.

10.**"Coordinating National Operating System with Cloud Computing; Second Phase of Zamin Started,"** *Mehr News Agency,* December 31, 2013, http://www.mehrnews.com/TextVersionDetail/2066094.

11.**"Legal VPNS to Be Soon Available,"** *Mehr News Agency,* February 5, 2013*,*

http://www.mehrnews.com/detail/News/1800539.

12. http://www.vpn.ir

13.**"Access to TOR Blocked: A New Step Towards Restricting Safe Access to the Internet?"** *International Campaign for Human Rights in Iran,* July 31, 2014, http://persian.iranhumanrights.org/1393/05/tor-ban/.

14.**"Khorramabadi: Five Million Websites Have Been Filtered,"** *Mehr News Agency,* November 18, 2008, http://old.mehrnews.com/fa/NewsDetail.aspx?NewsId=784979.

15.**"What Happened for WeChat to be Filtered?!,"** *Khabaronline,* January 16, 2014, http://www.khabaronline.ir/detail/329450/ict/comunication.

16. http://cyber.police.ir/

17.**"Blogger Dies in Detention, Torture Suspected,"** *International Campaign for Human Rights in Iran* November 8, 2012, http://www.iranhumanrights.org/2012/11/sattar-beheshti/.

18.**"Illegal Pressure by Cyberpolice on an Internet Provider to Reveal Personal Information of Its Customer,"** *International Campaign for Human Rights in Iran,* April 22, 2014, http://persian.iranhumanrights.org/1393/02/bayan-fata/.

19.http://www.ircarmy.com/ - http://www.hcarmy.net/ .

20.**"Eleven Internet Professionals Sentenced to One to Eleven Years in Prison,"** *International Campaign for Human Rights in Iran,* June 20, 2014, http://www.iranhumanrights.org/2014/06/cyber-activists/ .

21.**" Acknowledge Sattar Died In the Hands of His Interrogator, Demands Beheshti Lawyer,"** *International Campaign for Human Rights in Iran,* June 27, 2013, http://www.iranhumanrights.org/2013/06/sattar_beheshti-5/.

22. **Mohammad Hadi Sohrabi-Haghighat, "New Media and Social-political Change in Iran,"** *Cyber Orient* 5, no. 1 (2011)*,* http://www.cyberorient.net/article.do?articleId=6187.

23.**"Regulations for Information and News Websites,"** *Islamic Parliament Research Center,* November 6, 2001, http://rc.majlis.ir/fa/law/show/100746.

24.**"Formation of the Committee to Determine Illegal Websites,"** *Islamic Parliament Research Center,* December 31, 2002, http://rc.majlis.ir/fa/law/show/101083.

25.**"Making the Cyberspace Healthy in Addition to Technical Filtering,"** *Aftab Website,* July 23, 1999, http://goo.gl/8ig1cQ.

26.**"Iranian journalist faces manslaughter charge,"** Journalism.co.uk, May 9, 2003, http://www.journalism.co.uk/news/iranian-journalist-faces-manslaughter-charge/s2/a5635/.

27.**"Four Journalists Sentenced to Prison, Floggings,"** *International Campaign for Human Rights in Iran,* February 10, 2009, http://www.iranhumanrights.org/2009/02/journalistssentenced/.

28.**"Regulations for Organization of Internet Websites,"** http://samandehi.ir/samHelp/regulation.html.

29.**"Computer Crimes Law,"** http://internet.ir/law.html.

30.**"List of Instances of Criminal Content on the Internet,"** http://internet.ir/crime_index.html.

31.**"Establishment of the Supreme Cyberspace Council by the Order of the Supreme Leader,"** *Mehr News Agency,* March 7, 2012, http://old.mehrnews.com/fa/NewsDetail.aspx?NewsId=1554270.

32.**"Heard the One about the President?"** *The Guardian,* April 13, 2006, http://www.theguardian.com/world/2006/apr/14/iran.topstories3.

33.**"Khorramabadi: Five Million Websites Have Been Filtered,"** *Mehr News Agency,* November 18, 2008, http://old.mehrnews.com/fa/NewsDetail.aspx?NewsId=784979.

34.**"Officials Express their Views on Filtering of WhatsApp,"** *Iranian Students News Agency, April 4, 2014,* http://goo.gl/RSJRHO.

35.**"Design of an Iranian Software Similar to Viber,"** *ITanalyz.ir,* September 13, 2014,

http://itanalyze.com/news/2014/09/13/25955.php

36. **"Rouhani Orders to Stop Filtering of WhatsApp Social Network,"** *Alef,* May 6, 2014,

http://alef.ir/vdcjtie8muqe8xz.fsfu.html?225436.

37. **"President can not Prevent the Actions of the 'Committee to Determine Instances of Criminal Content on the Internet'; Claim of the Communications Minister is False,"** *Fars News Agency,* May 4, 2014,

http://www.farsnews.com/newstext.php?nn=13930214000858.

38.**"Ejei: Avoidance of the Communications Ministry to Implement Blocking of WhatsApp is Against the Law,"** *RadioFarda,* May 20, 2014, http://www.radiofarda.com/content/f10-judiciary-ejei-telecommunication-ministry-whatsapp-filtering/25390866.html.

39.**"Mobile Apps Are Not Presently Filtered,"** *ITanalyze.ir,* June 18, 2014, http://itanalyze.com/news/2014/06/18/25170.php.

40.**"Officials Express their Views on Filtering of WhatsApp,"** *Iranian Students News Agency,* April 4, 2014, http://goo.gl/RSJRHO.

41.**"Obtaining Permits for Mobile Apps Becomes Obligatory,"** *Mehr News Agency,* February, June 18, 2014, http://www.mehrnews.com/TextVersionDetail/2239758.

42.**"Interview with the Minister of Communications: National Internet will Be Operational in August,"** *Fars News Agency,* July 27, 2014, http://www.farsnews.com/newstext.php?nn=8505010040.

43.**"Twenty Fold Increase in Internet Speed with Implementation of the National Internet,"** *Students News,* May 26, 2014, http://snn.ir/print/317764.

44.**"Fifth Five Year Development Plan of the Islamic Republic of Iran (1390-1394),"** *Islamic Parliament Research Center,* http://rc.majlis.ir/fa/law/show/790196.

45.**"Recommendations received by Iran (Islamic Republic of),"** *UPR Info,* http://www.upr-info.org/en/review/Iran-%28Islamic-Republic-of%29.

46.**"Ahmadi Moghaddam: Google Search Engine is a Spying Tool,"** *Mehr News Agency,* January 10, 2012*,* http://old.mehrnews.com/fa/NewsDetail.aspx?NewsId=1506089.

47.**"40 Billion Tomans Spent on Creation of National Data Centers,"** *Khabaronline,* May 21, 2012*,*

http://khabaronline.ir/detail/214889/ict/5121.

48.**"National Data Centers: A plan from Yesterday until Tomorrow,"** *IT News Agency,* November 10, 2012, *http://www.itna.ir/vdcceiqi.2bq0o8laa2.html.*

49.**Website of the Center for Issuance of SSL Certificates,** http://www.enamad.ir.

50.**"Issuance of 100,000 Electronic Signature Certificates,"** *ITanalyze.ir,* March 16, 2014*,* http://itanalyze.com/news/2014/03/16/24205.php.

51.**Ibid**.

52.**"Iran's New Methods of Internet Filtering Put Users At Risk,"** *International Campaign for Human Rights in Iran, February 3, 2014,* http://www.iranhumanrights.org/2014/02/internet-ssl/.

53.**"Development of the National Operating System,"** *ITanalyz.ir,* http://itanalyze.com/archives/N-OS.pdf.

54.**"Document for the National Operating System Adopted,"** *Aftab News,* April 28, 2010, http://goo.gl/KR0ATI.

55.**"Coordinating National Operating System with Cloud Computing; Second Phase of Zamin Started,"** *Mehr News Agency, December 31, 2013,* http://www.mehrnews.com/TextVersionDetail/2066094.

56.**"Government Bans Use of Windows; Linux is Approved,"** *Islamic Republic of Iran News Network,* September 9, 2013, http://goo.gl/b2zTsS.

57.**"Details of the National Search Engine: Ya Hagh to Replace Google and Yahoo,"** *August 28, 2010*

http://old.mehrnews.com/fa/NewsDetail.aspx?NewsId=1141606.

58.http://facenama.com/home?v=1.

59.http://facekoob.ir/.

60.**"Email Becomes National Through Compulsion,"** *Trade Organization of Internet Guilds,* May 12, 2012, http://goo.gl/l45csj.

61.**"Legal VPNS to Be Soon Available,"** *Mehr News Agency,* February 5, 2013,

http://www.mehrnews.com/detail/News/1800539.

62.**"Infrastructure Executive Talks about Why Legal VPN Project Failed,"** July 17, 2013, http://www.aparat.com/v/xHpgw

63.**"Bill to Ban VPNs Would Cut Internet Access,"** *International Campaign for Human Rights in Iran,* May 14, 2014, http://www.iranhumanrights.org/2014/05/vpn-bill/.

64.**"National Internet Enters Service Phase,"** *90ICT,* April 21, 2014, http://www.90ict.com/index.aspx?pid=99&articleid=50346.

65.**"Communications Minister: National Internet Network Will Become Operational in 2015,"** *Fars News,* November 30, 2013, http://farsnews.com/newstext.php?nn=13920925001347.

66.**"17 Billion Dollars Invested by the Government for the National Internet Network,"** *Tasnim News Agency,* February 17, 2014, http://www.tasnimnews.com/home/single/285728.

67.**"Online Activities of All Users Are Monitored,"** *Dana News Agency,* February 15, 2014,

International Campaign for Human Rights in Iran, May 14, 2014, http://goo.gl/dNk6RW.

68.**Ibid**.

69.**"Cyber Police Begins Work,"** *Donya-e Eqtesad Newspaper,* January 24, 2011, http://www.donya-e-eqtesad.com/news/640615/.

70.**"Newly Disclosed Medical Examiner Report Confirms Sattar Beheshti Died of Internal Bleeding,"** *International Campaign for Human Rights in Iran,* November 11, 2013, http://www.iranhumanrights.org/2013/11/sattar-beheshti-2/.

71.**"In Exclusive Interview Commander Jalili Says Garrison for Cyber Warfare to Be Established,"** *Bultannews,* March 6, 2011, http://goo.gl/IwDxLV.

72.**“Basij Organization Head: Attacks and Hackings Are the Work of the Revolutionary Guards Cyber Army,”** *Digarban,* March 13, 2011, http://digarban.com/node/659.

73.**“Commander of the Ali-inb-Abitaleb Qum Gaurds: The Guards Have Formed the Second Cyber Army in the World,”** *Fars News Agency,* May 20, 2010, http://www.farsnews.com/newstext.php?nn=8902300353.

74.**“An Iranian Government Official Doubts the Existence of the Revolutionary Guards’ Cyber Army,”** *BBC Persian,* September 6, 2011, http://www.bbc.co.uk/persian/iran/2011/09/110906_l39_mehdi-sarami_iran_cyber_armi.shtml.

75.**“Radio Zamaneh Website Hacked,”** *BBC Persian,* January 30, 2010, http://www.bbc.co.uk/persian/iran/2010/01/100130_u02-radiozamaneh-hackers.shtml.

76.**“'Iranian Cyber Army' uilding Botnet with Exploit Kit,”** *ZDNet,* October 26, 2010, http://www.zdnet.com/blog/security/iranian-cyber-army-building-botnet-with-exploit-kit/7561.

77.**“Eleven Internet Professionals Sentenced to One to Eleven Years in Prison,”** *International Campaign for Human Rights in Iran,* June 20, 2014,

http://www.iranhumanrights.org/2014/06/cyber-activists/.

78.**“Several Anti-Regime Sites Hacked by the Revolutionary Guards,”** *Mashregh News,* January 30, 2014, http://goo.gl/Rv5Nd1.

79.**“Four Student Cyber Activists Detained in Tehran and Mashad,”** *JARAS,* January 30, 2014, http://www.rahesabz.net/story/79977/ .

80.**Ibid**.

81.**“Ruling of Combined 127-Year Sentence for Facebook Users Violates Iran’s Own Laws,”** *International Campaign for Human Rights in Iran,* August 27, 2014, http://www.iranhumanrights.org/2014/07/fb-127-yrs/ .

82.**“Sentencing of Eight Facebook Users Charged with Collusion Against the National Security,”** *Islamic Republic News Agency,* July 13, 2014, http://goo.gl/pRaz0q.

83.**“Full transcript of Ann Curry's interview with Iranian President Hassan Rouhani,”** *NBC News,* September 9 ,2013, http://www.nbcnews.com/id/53069733/ns/world_news-mideast_n_africa/t/full-transcript-ann-currys-interview-iranian-president-hassan-rouhani/#.Us37V7R8C8w

84.**“Restrictions on Internet Access and Mobile Apps Grow During Rouhani Administration,”** *International Campaign for Human Rights in Iran,* January 9, 2014, http://www.iranhumanrights.org/2014/01/rouhani-internet/.

85.**“Jannati: I Do Not Consider Membership in Facebook a Crime; I am a Member,”** *Fars News Agency,* November 15, 2013 http://www.farsnews.com/newstext.php?nn=13920824000069.

86.**“Communications Minister: We Can Manage Facebook inside the Country,”** *Asr Iran News,* May 1, 2014, http://goo.gl/wOVbph.

87.**“Alam-alHoda Warns Against Lifting Facebook Filtering,”** *Tabnak News,* May 2, 2014, http://goo.gl/MG4Tpz.

88.“**Minister of Guidance: Facebook Should Be Available to Everyone; Filtering of Websites Must Be Minimal,”** *Mehr News Agency,* November 5, 2013, http://www.mehrnews.com/detail/news/2169418.

89.**Ibid**.

90.**“Rouhani battles judiciary over Internet censorship,”** *Al-Monitor,* May 28, 2014, http://www.al-monitor.com/pulse/originals/2014/05/iran-rouhani-battled-judiciary-internet-censorship.html.

91.**“Rouhani: I Am Not Satisfied with Internet Bandwidth in the Country,”** *Aftab News Agency,* May 17, 2014, http://aftabnews.ir/fa/news/244235.

92.**“RighTel Has 1.5 Million Subscribers,”** *Islamic Republic News Agency,* August 30, 2013, http://goo.gl/v7NCuk.

93.**“Statistics for the Iran Communications Company,”** http://tci.ir/s40/page5.aspx?lang=Fa.

94.**“Grand Ayatollah Issues Fatwa Stating High Speed Internet is against Sharia,”** *International Campaign for Human Rights in Iran,* August 27, 2014, http://www.iranhumanrights.org/2014/08/makarem-internet/.

95.**“Rouhani: We Can Not Shut the Doors of the Outside World to Our Youth,”** *Islamic Students News Agency,* September 1, 2014, http://goo.gl/BbD5dX.

96. **"Tender Number 93/10 for Development of Fiber Optics Network Infrastructure,"** http://www.tic.ir/fa/tender/302.

97.**Special Report on Internet Surveillance, Focusing on 5 Governments and 5 Companies: Enemies of the Internet,"** *Reporters Without Borders,* 15 March, 2013, http://en.rsf.org/special-report-on-internet-11-03-2013,44197.html.

98.**"UN Human Rights Council Reaffirms Promotion and Protection of Human Rights Online,"** *Electronic Frontier Foundation,* July 1, 2014, https://www.eff.org/deeplinks/2014/07/un-human-rights-council-reaffirms-promotion-and-protection-human-rights-online.

99.**Constitution if the Islamic Republic of Iran,** http://en.wikipedia.org/wiki/Constitution_of_the_Islamic_Republic_of_Iran.

INTERNATIONAL CAMPAIGN FOR HUMAN RIGHTS IN IRAN

www.iranhumanrights.org

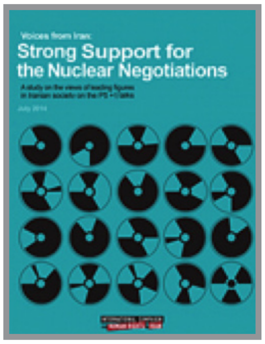
Internet in Chains

The Front Line of State Repression in Iran

Internet in Chains: The Front Lines of State Repression in Iran presents an in-depth examination of the Iranian government's intensifying efforts to censor and control the Internet. The report presents a detailed analysis of the technological and policy initiatives underway in Iran—including development of the country's National Information Network and all of its various components, the state's filtering activities, especially with regard to mobile applications, and the intensifying prosecution of Internet professionals and activists in Iran. It reveals the tools, methods, and capabilities that are significantly increasing the state's ability to control access to the Internet inside Iran, and to monitor, undetected by the user, online communications.

Recent reports

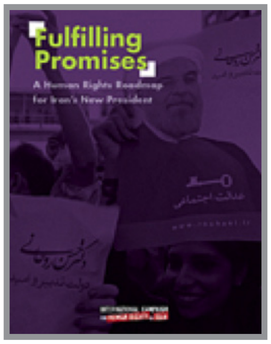
by the International Campaign for Human Rights in Iran



Voices from Iran:
Strong Support for
the Nuclear Negotiations

Voices from Iran: Strong Support for the Nuclear Negotiations

(July 2014)



Fulfilling
Promises
A Human Rights Roadmap
for Iran's New President

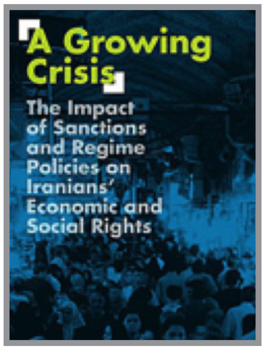
Fulfilling Promises: A Human Rights Roadmap for Iran's New President

(August 2013)

Iran's State TV:
A Major
Human Rights Violator
IRIB Briefing Paper

Iran's State TV: A Major Human Rights Violator

(July 2014)



A Growing
Crisis
The Impact
of Sanctions
and Regime
Policies on
Iranians'
Economic and
Social Rights

A Growing Crisis: The Impact of Sanctions and Regime Policies on Iranians' Economic and Social Rights

(April 2013)

INTERNATIONAL CAMPAIGN
FOR HUMAN RIGHTS IN IRAN

www.iranhumanrights.org