Report

Guards at the Gate

The Expanding State Control Over the Internet in Iran

Center for HUMAN RIGHTS in Iran

Guards at the Gate
The Expanding State Control Over the Internet in Iran

Center for Human Rights in Iran
New York
Tel: +1 -347-689-7782

www.iranhumanrights.org

Guards at the gate

The Expanding State Control Over the Internet in Iran

January 2018

Center for HUMAN RIGHTS in Iran

www.iranhumanrights.org

Table of Contents

Center for HUMAN RIGHTS in Iran

About us

The **Center for Human Rights in Iran (CHRI)** is an independent, nonpartisan, nonprofit organization dedicated to the protection and promotion of human rights in Iran. CHRI 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 and videos, and work to build support for human rights inside Iran as well. CHRI 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.

Executive Summary

Guards at the Gate: The Expanding State Control Over the Internet in Iran by the Center for Human Rights in Iran (CHRI), examines the key policy and technological developments regarding the internet in Iran over the 2013-2018 period. The report reveals the steady progress the Iranian government has made in controlling its citizenry's use of the internet. During the unrest that swept through Iran on the eve of 2018, the authorities implemented major disruptions to internet access through slowdowns and the blocking of circumvention tools, blocked the Instagram social media platform and the Telegram messaging app heavily used by the protesters to mobilize the street protests, and briefly cut off Iranians' access to the global internet on December 30, 2017, demonstrating a new level of technical sophistication. These actions confirm the main contention of this report—namely, that while internet use has expanded throughout Iran with the help of upgrades to the country's telecommunications infrastructure and faster and cheaper internet service, key technological initiatives undertaken by the Iranian government, in particular development of Iran's state-controlled National Internet Network (NIN), have significantly enhanced the government's ability to restrict, block and monitor internet use in Iran.

Over the period this report covers, which encompasses President Rouhani's first term (2013-2017) and the beginning of his second, internet use has grown robustly in Iran. According to the UN's International Telecommunication Union (ITU), 53 percent of the country's 80 million-plus population use the internet, which may well be an under-estimate. With 3G and 4G service made widely available by the Rouhani administration, tens of millions of Iranians now access the internet and social media on the 40 million mobile phones now in use in the country. Messaging applications such as Telegram serve as a major platform for societal discussion of political, social and cultural issues. Online communication has become particularly central to Iran's young, educated and tech savvy population, with the internet increasingly eclipsing traditional print and broadcast media to become the most significant "public square" in Iran.

Yet while internet use has increased and its centrality to Iranian discourse has grown exponentially—and the Rouhani administration has facilitated this greater use by increasing internet speeds and lowering access costs in Iran—internet control, censorship and surveillance by the state have also expanded significantly.[1] This is largely due to the development of the NIN, which has accelerated under the Rouhani administration. The NIN's national search engines now systematically filter key words and phrases—and send users to sites that deliver only state-approved and sometimes fabricated content. NIN tools and services facilitate the state's ability to identify users and access their online communications, deeply compromising user privacy and security. The government steers Iranians toward use of the NIN and its search engines, security certificates, email services and video broadcasting services through price and internet speed incentives, violating net neutrality principles. Critically, the NIN's ability to separate domestic internet traffic in Iran from international internet traffic now allows, for the first time, the state to

cut Iranians off from the global internet while maintaining access to domestic online sites and services.

The capacity to restrict the people of Iran to state-approved content on a domestic internet has been a long-standing goal of hardliners in Iran—intelligence and security agencies, judicial officials, and the country's supreme leader, Ali Khamenei, who fear internet freedom and view the internet as a Western ploy to undermine the Islamic Republic. With the demonstrated capacity to sever Iranians' access to the global internet while maintaining the availability of Iran's state-controlled internet, this goal has now been realized, justifying for them the huge investment the Iranian government has made in the development of the NIN.

In addition, during this period the government's blocking of major social media sites such as Twitter, Facebook and YouTube, as well as millions of other websites, has continued, even as Rouhani has on a few occasions thwarted the blocking of messaging applications such as WhatsApp. Moreover, intensifying state filtering is now increasingly targeting applications that provide encryption by default (which provide security automatically, without user input), that are vital to Iranians' efforts to maintain online privacy. State-sponsored hacking attacks—DDoS attacks, phishing, malware, message interception and the use of insecure fake applications—have also multiplied. With hardline state security and intelligence organizations in control of the country's telecommunications infrastructure, their ability to access private online communications, unhindered by any judicial oversight, poses grave threats to Iranian users; individuals are arrested and sentenced to lengthy prison terms on the basis of online content unlawfully obtained by the state in this manner.

Rouhani has been silent in the face of these attacks, despite his stated support for internet freedom and his promulgation of a citizens' rights charter. Indeed, Rouhani has proved either unable or unwilling to defend internet freedom, and, in some respects, such as in the accelerated development of the NIN, has significantly facilitated and implemented decisions and initiatives that severely violate it. The recent brief severance of access to the global internet and the blocking of Telegram and Instagram are a huge departure from his statements after his re-election in 2017 against filtering and his pledges to protect Iranians' online connection to the world.

The state has significantly deepened its control over cyberspace in Iran. As the NIN has progressed toward the final stages of implementation, it has become clear that the government's development of a national network that provides faster and cheaper internet access has also led to the creation of a technical infrastructure that can more effectively block, censor, spread false information, and access Iranian users' online communications, and it has made the Iranian citizenry highly vulnerable to the state intelligence organizations that control this technical infrastructure. Internet freedom is under assault in Iran, and the rights of the Iranian people to information access and internet privacy, both integral to the fundamental right of freedom of expression, are being severely violated.

Recommendations

To the Rouhani administration

- The Rouhani administration should pledge not to cut off or disrupt in any way Iranians' access to the global internet, and it should not allow its Ministry of Communications and Information Technology (hereafter referred to as the Ministry of Communications) to implement any disruption to such access for any reason.

- In line with net neutrality principles, the Ministry of Communications should allow internet traffic to flow without discrimination, restriction or interference, regardless of the sender, receiver or type of content, in order to ensure users' freedom of choice, and it should end the discriminatory practice of selectively applying higher speeds and lower fees to domestic websites on Iran's National Information Network.

- The administration should submit a bill to Parliament bringing these net neutrality principles into Iran's body of law, giving permanence to them so they are not dependent on the proclivities of individual administrations.

- The Ministry of Communications should publish the conditions under which security agencies may access users' online information and the explicit requirement that this be done only in accordance with these conditions and the law, and pledge not to honor any request for access to Iranian users' accounts by the judiciary or intelligence and security organizations that violates these rules and regulations.

- The administration should introduce a bill to Parliament protecting online communications between citizens on national and international networks, and clarify and codify the prohibition of unlawful access by judicial and intelligence agencies.

- The Ministry of Communications should stop implementing the filtering of websites, online services and applications that provide encryption by default, which are used to safeguard online privacy worldwide.

- The Ministry of Communications should stop implementing the filtering of online content that violates international standards of freedom of speech, as delineated by the International Covenant on Civil and Political Rights (ICCPR), of which Iran is a signatory, including websites engaged in news, education, services, culture, sports or belonging to political opponents and critics and their followers inside Iran; and it should make a determined effort to remove filters on social media networks which have been unlawfully blocked in Iran, such as Twitter, Facebook and YouTube.

- The Ministry of Communications should stop implementing the filtering of content based on key words searches in Iran's national search engines that violate ICCPR rights, and it should stop sending users to fabricated sites designed to deliver false and defamatory content.

- The administration should introduce a bill to Parliament codifying the above filtering regulations and prohibiting the deletion of content from websites.

To the Iranian Parliament

- The Iranian Parliament should pass legislation supporting and protecting online personal privacy from unauthorized state access and observing the principles of net neutrality.

- The Law on Cyber Crimes, passed by Parliament in 2009, does not protect civil rights and individual privacy. Its vague language gives judicial and security agencies an open hand to violate the privacy of individuals. Legislators should revise the law to ensure compliance with domestic laws and international commitments guaranteeing privacy.

- Parliament should rescind the aspects of Iran's Law on Computer Crimes that violate citizens' right to freedom of expression, specifically articles H and T which list various examples of criminal content, as these articles violate the ICCPR's right to free speech.

- The Law on Computer Crimes should be revised so as to guarantee that no individual or state agency would have the right to use the country's communications infrastructure to intercept messages containing password verification information.

To the Iranian judiciary

- The judiciary should publish a list of clear and specific rules and regulations regarding state access to accounts.

- The judiciary should not request, pressure or in any way use its authority to enable or approve unlawful state access to accounts.

To the UN and the special rapporteurs

- The United Nations should continue to hold Iranian officials responsible for hacking conducted by state agencies with access to the country's

- communications infrastructure, by issuing public statements condemning such activities, incorporating relevant documentation in their reports, and directly calling for the cessation of such activities in public forums and in private dialogue with Iranian officials.

- The UN special rapporteur on the situation of human rights in Iran and the UN special rapporteur on the right to freedom of opinion and expression should include in their reports instances of Iranian state violations of freedom of expression, the right to access information and the right to privacy, and other violation of rights in online communications in Iran.

- The UN special rapporteurs on human rights in Iran and on freedom of expression should investigate the role of any company selling advanced equipment to Iranian state agencies engaged in surveillance against civil and political activists. As long as there are no guarantees for the protection of citizens' rights, such sales could result in serious violations of the right to privacy of Iranian citizens.

To member states

- Member states of the UN, in particular, members of the European Union that are engaged with Iran on building diplomatic and business relationships, should express their concerns directly to their Iranian counterparts regarding violations of internet access and privacy in Iran, and express clearly and forcefully the unacceptability of state-sponsored hacking of Iranians' accounts who are living abroad in those countries.

To technology companies

- Technology companies should remove restrictions on the sale and/or download of personal communication tools, services and products, allowing Iranian citizens full access to the latest technologies to protect online access, privacy and security.

- Technology companies should assure their Iranian users that they will take no action that will compromise their online privacy, for example, they will not place their servers or user data inside Iran, regardless of requests by the Iranian government.

- Technology companies active in Iran should inform the public through accessible, detailed and transparent reports of any agreements they make with the Iranian government that may potentially affect internet access or privacy in Iran.

- Technology companies should refuse to agree to any demands made by the Iranian government for online censorship that violate Iranians' fundamental right to freedom of speech.

To internet freedom organizations

- Internet freedom organizations should create Farsi-language channels to communicate directly with the Iranian citizenry (for example, via Telegram or Twitter accounts) to deliver information on: tools and services to circumvent state filtering and facilitate internet access, privacy and security; tools and methods of state-sponsored hacking in Iran to facilitate more effective preventative and protective measures; and on the development of customized tools to protect Iranians' security and privacy.

Methodology

This report by the Center for Human Rights in Iran (CHRI) incorporates independent and original research undertaken by CHRI's internet security researchers and analysts during the period from January 2017 to January 2018. CHRI conducted detailed technical analysis of Iran's National Internet Network (NIN) and its various tools and services, including the national operating systems, browser, search engines, emails services, mobile applications, and other software; the tools and methods used in state-sponsored hacking attacks (DDoS, phishing, malware, message interception and fake applications); and the accounts of state-sponsored hacking victims. CHRI also incorporated extensive interviews with approximately 26 Iranian information and communications technology professionals, journalists, activists and other members of civil society in Iran who have been the victims of state-sponsored hacking attacks. The interviews were done via secure online platforms during the period from February 4, 2017 to February 14, 2017. CHRI also undertook a comprehensive review of Iranian state policy, legislation and practices regarding internet access, censorship, surveillance, cyberattacks and the development of Iran's National Internet Network, as well as public statements by Supreme Leader Ali Khamenei, President Rouhani, his cabinet and other administration officials, Parliamentarians, judicial officials, Islamic Revolutionary Guard Corps' (IRGC) members, and leading state-affiliated clerics, as reported in the Iranian press and on the websites of those officials. CHRI also consulted with leading international internet freedom researchers.In particular, CHRI wishes to thank Collin Anderson, a Washington, DC–based researcher focused on cybersecurity and internet regulation, for his review of and assistance with this report. This report incorporates the research contained in, and is a follow up to, CHRI's November 2014 report, "Internet in Chains": The Front Line of State Repression in Iran.[2]

Introduction

Guards at the Gate: The Expanding State Control Over the Internet in Iran by the Center for Human Rights in Iran (CHRI), provides a detailed analysis of internet policy and technological developments in Iran over the 2013-2018 period. The report, which builds on CHRI's research and reporting on internet freedom and security issues in Iran and the growing technological capabilities of the state throughout these years, reveals the steady progress the Iranian government has made in controlling its citizenry's use of the internet. In particular, ***Guards at the Gate*** examines the development of the country's state-controlled National Information Network (NIN) and the enhanced state capabilities for internet filtering, blocking and surveillance it has enabled. The report assesses the implications of these developments for Iranians' access to information and online privacy, and offers recommendations to the authorities in Iran and to the international community to address the rights violations Iranians are being subjected to by Iran's internet policies.

53 percent of the country's 80 million people use the internet and there are 40 million mobile phones in use in the country.

During the unrest that swept through Iran on the eve of 2018, the authorities implemented major disruptions to internet access through slowdowns and the blocking of circumvention tools, blocked the Instagram social media platform and the Telegram messaging app used heavily by the protesters to mobilize the street protests, and briefly cut off Iranians' access to the global internet on December 30, 2017, demonstrating a new level of technical sophistication. These actions confirm the main contention of this report—namely, that while internet use has expanded throughout Iran with the help of upgrades to the country's telecommunications infrastructure and faster and cheaper internet service, technological initiatives undertaken by the Iranian government, in particular development of Iran's NIN, have significantly enhanced the government's ability to restrict, block and monitor internet use in Iran.

Over the period this report covers, which encompasses President Rouhani's first term (2013-2017) and the beginning of his second, internet use in Iran has grown exponentially. Some 53 percent of the country's 80 million-plus people use the internet, according to the UN's International Telecommunication Union (ITU), which may well be an underestimate given that there are now over 40 million mobile phones in use in the country and the Telegram messaging application alone has 40 million registered users in Iran. Election campaigns are increasingly waged on Telegram, Twitter and Instagram; social media networks serve as major platforms for Iranians to discuss political, social and cultural issues; and mobile applications are being rapidly developed for business start-ups. Online communication has become particularly central to Iran's youth. Sixty percent of the country's population is under 30, and they are an educated and tech savvy population that has produced a vibrant and entrepreneurial tech community.

This increase in internet use has been propelled by the Rouhani government's decision to lift the long-standing limitations on internet speeds in Iran. Rouhani has increased bandwidths across the country, and expanded the availability of 3G and 4G licenses, which lay the groundwork for the exponential increase in mobile phone

use. This increase in speed has affected all aspects of Iranian society. It allows the transfer of large files, video streaming, the use of VoIP (Voice over Internet Protocol, used in messaging applications such as Telegram, Signal and WhatsApp) and other services that aid information sharing. This has not only facilitated general communication amongst the public, higher internet speeds have enhanced professional, academic and commercial communications, as well as the ability to develop Iranian online services. It has also been critical to the work of journalists, activists and other members of civil society in Iran.

The state too has a heavy presence on the internet, with Iranian officials themselves avid users of the same online platforms that they block for the Iranian general public. They use Twitter, Telegram, Facebook and other platforms to promote their own narratives of issues and events, recognizing that the internet is increasingly eclipsing traditional print and broadcast media in Iran. The authorities have also seen that it has proven harder to establish the kind monopoly on information on the internet that it has enjoyed on the country's print and broadcast media.

"We must, God willing, follow this [NIN] project so we won't sustain irreparable blows."

Iran's Supreme Leader, Ayatollah Ali Khamenei, September 2016

As a result, Iranian state policies and technical initiatives have increasingly focused on strengthening the state's capabilities for internet control, censorship and surveillance. The centerpiece of these efforts has been the accelerated development of the country's NIN. During Rouhani's tenure, many aspects of the NIN and its various tools and services—national search engines, data centers, email and video services and the likes—have become operational.

As will be detailed in this report, the NIN and its various components significantly expand the state's capabilities to control the internet in Iran. The NIN's national search engines now systematically filter key words and phrases—and send users to sites that deliver only state-approved and sometimes fabricated content. NIN tools and services facilitate the state's ability to identify users and access their online communications, deeply compromising user privacy and security. The government steers Iranians toward use of the NIN through price and internet speed incentives, violating net neutrality principles. Critically, the NIN's ability to separate domestic internet traffic in Iran from international internet traffic now allows, for the first time, the state to cut Iranians off from the global internet while maintaining access to domestic online sites and services—a capacity demonstrated briefly on December 30, 2017. Indeed, Iranian officials view the NIN as the central means to enhance state control over the internet, a goal promoted by Iran's supreme leader, Ali Khamenei. In a meeting with President Rouhani and his cabinet in September 2016, Khamenei said, "We must, God willing, follow this project so we won't sustain irreparable blows."[3]

The capacity to restrict the people of Iran to state-approved content on a domestic internet has been a long-standing goal of hardliners in Iran—intelligence and security agencies, judicial officials, and the country's supreme leader, Ali Khamenei—who fear internet freedom and view the internet as a Western ploy to undermine the Islamic Republic. The government's disruption to internet access in Iran during the 2009 protests, prior to the development of the NIN, showed that any internet disruption also severed the government and other critical agencies

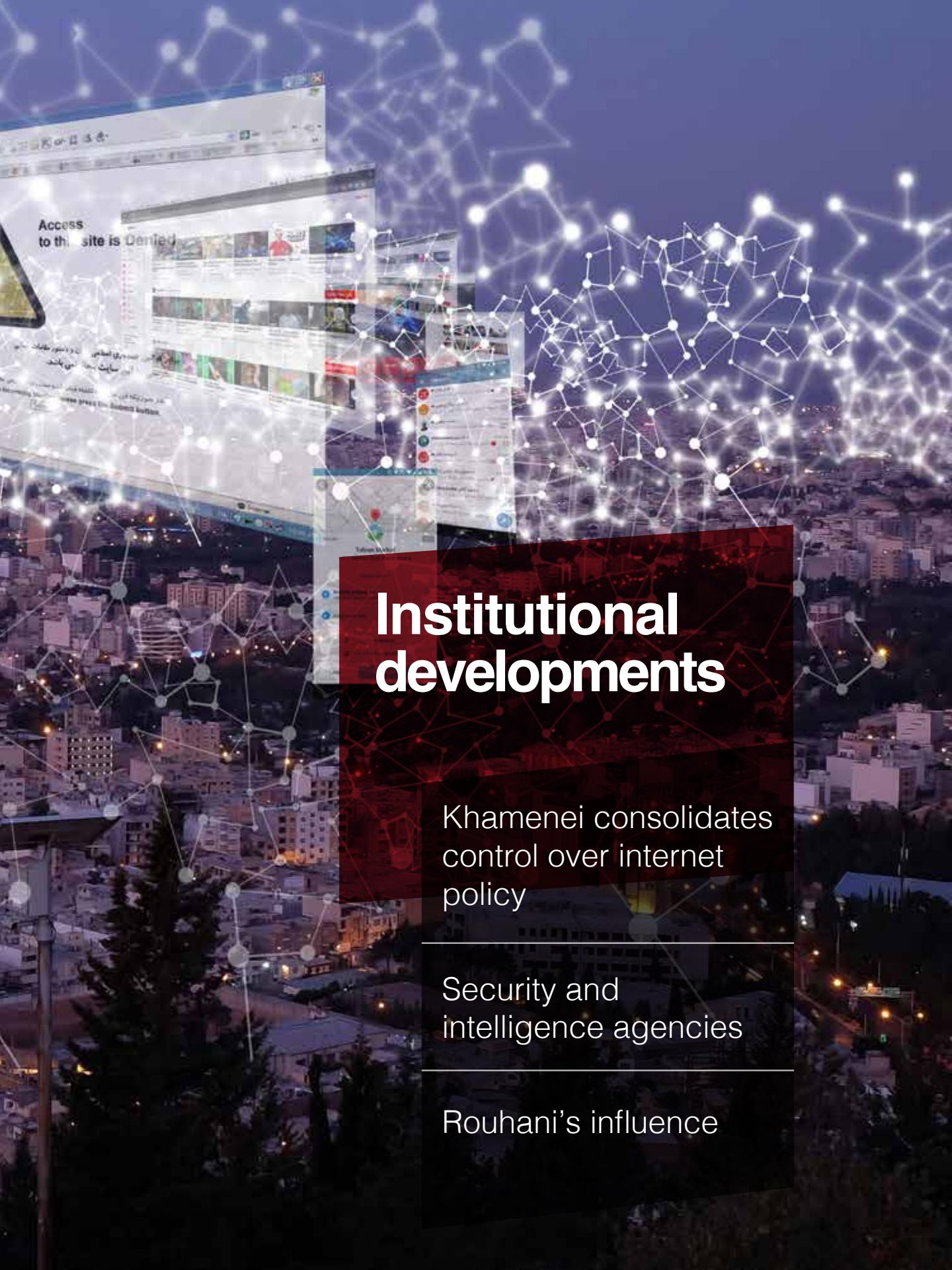
from needed online communications. With the NIN's ability to separate global from domestic internet traffic, the state's goal of severing Iranians' access to the global internet while maintaining the availability of Iran's state-controlled domestic internet—thereby restricting Iranians, as needed and at the government's discretion, to state-approved content—has now been realized. This alone has justified for them the major decade-long investment the Iranian government has made in the development of the NIN.

In addition, during this period the government's blocking of major social media sites such as Twitter, Facebook and YouTube, as well as millions of other websites, has continued, even as Rouhani has on a few occasions thwarted the blocking of messaging applications such as WhatsApp. Moreover, intensifying state filtering is now increasingly targeting applications that provide encryption by default (which provide security automatically, without user input), that are vital to Iranians' efforts to maintain online privacy.

Iranian security and intelligence organizations have also intensified cyberattacks against the citizenry, bringing down websites and hacking into personal accounts in order to identify and block voices critical of state policy. Indeed, state-sponsored DDoS attacks, phishing, malware, message interception and the use of insecure fake applications have notably increased under Rouhani's administration. With hardline state security and intelligence organizations in control of the country's telecommunications infrastructure, their ability to access private online communications, unhindered by any judicial oversight, poses grave threats to Iranian users; individuals are arrested and sentenced to lengthy prison terms on the basis of online content unlawfully obtained by the state in this manner.

Rouhani has remained publicly silent in the face of these attacks and has made no public effort to advance judicial or legislative oversight of state access to accounts or to otherwise defend the online privacy that is ostensibly protected by Iranian law, despite his stated support for internet freedom and his promulgation of a citizens' rights charter. Overall, Rouhani has proved either unable or unwilling to defend internet freedom, and, in some respects, such as in the accelerated development of the NIN, has facilitated and implemented decisions and initiatives that severely violate it. The recent brief severance of access to the global internet and the blocking of Telegram and Instagram are a huge departure from his statements after his re-election in 2017 against filtering and his pledges to protect Iranians' online connection to the world.

Guards at the Gate provides a comprehensive understanding of the significant technological advancements the Iranian government has made over the last five years, and the implications these new capabilities have for Iranians' access to the internet and their ability to communicate privately and safely online. The dream of hardliners in Iran—the ability to restrict its citizens' engagement with the outside world and prevent exposure to information that challenges their world view—is becoming a reality. In the process, the Iranian people's rights to information access and internet privacy, both integral to the fundamental right of freedom of expression, are being severely violated.



Institutional developments

Khamenei consolidates control over internet policy

Security and intelligence agencies

Rouhani’s influence

Khamenei consolidates control over internet policy

Supreme leader Khamenei has sought to centralize control over internet policy under his authority.

Recognizing the significant role of digital communication in Iran, the country's supreme leader, Ayatollah Ali Khamenei, has increasingly sought to centralize control over the country's internet policy under his authority.

Toward this end, Khamenei centralized decision-making power over the internet in Iran's Supreme Council of Cyberspace. This 27-member body, formed on March 8, 2012 on Khamenei's orders, is chaired by Iran's president, but because all its individual members and most of those who represent organizational entities are handpicked by the supreme leader, the president and others from his cabinet who serve on the council have a more marginalized role in it. Indeed, this move significantly restricted the power of the president and his administration over internet policy, whose current members include many who favor a less restrictive online environment.

In a further consolidation, in 2015, several of the institutions that had been involved in internet policy making in the country were dissolved by order of Khamenei and merged into the Supreme Council of Cyberspace. Among these[4] were the Supreme Council of Informatics, which had been under the Management and Planning Organization; the Supreme Council of Information,[5] which was responsible for the production, refining and exchange of information, and monitoring the dissemination of information throughout the country (under the Interior Ministry); and the Supreme Council of Information Exchange,[6] which worked on various areas of vital systems security under Vice President Eshaq Jahangiri.

After the dissolution of these councils, their strategic, decision-making, monitoring and coordination responsibilities were transferred to the Supreme Council of Cyberspace.[7] The only body remaining outside the council is the Supreme Council of Information Technology, which changed its name to the Executive Council of Information Technology.[8] This council, which remained under Rouhani's direct authority, is responsible only for implementing the policies and decisions made by the Supreme Council of Cyberspace. With the new institutional configuration, significant authority and power was taken from the executive branch and transferred to institutions that are either directly controlled by Khamenei, who views the internet as a threat, or to institutions close to him through appointees, with grave implications for internet freedom and privacy in Iran.

Security and intelligence agencies

In addition to the Supreme Council of Cyberspace, other institutions play an important role in shaping internet policies and use in Iran—but they are similarly under the direct or indirect control of Khamenei.

The Working Group to Determine Instances of Criminal Content is the principal body charged with making internet filtering decisions. This group reports directly to the judiciary, whose head is under Khamenei's authority. The judiciary itself also has the power to shut down websites or applications, order the deletion of content, and order filtering, as does the country's cyber police. The cyber police are under the authority of Iran's national police, which reports to the Ministry of Interior. While that ministry is ostensibly under Rouhani's authority, as is the case with other ministries that are considered important to the country's security (such as the Ministry of Intelligence, the Ministry of Islamic Culture and Guidance, and the Ministry of Education), the head of the Ministry of Interior cannot be appointed without Khamenei's approval. Iran's Ministry of Islamic Guidance also can limit users' access to information.

Members of the Supreme Council of Cyberspace customarily visit the supreme leader to receive his advice on internet policies.

"Some agencies put a lot of pressure [on the Supreme Council] to disrupt the internet on the threshold of elections, or to block certain social media, but we opposed it."

Rouhani's former Minister of Communications Mahmoud Vaezi, February 26, 2016.

Yet it is direct interventions by Iran's security and intelligence agencies, in particular Iran's Islamic Revolutionary Guard Corps (IRGC), which also report directly to Supreme Leader Khamenei, that have come to play an increasingly important role in shaping the country's internet policies.[9]

For example, Iran's Telecommunications Company, which is owned by the IRGC, is one of the principal entities involved in the design and development of the National Information Network (NIN), Iran's state-controlled and censored internet, according to the NIN's documents on the Ministry of Communication's website.[10] In addition, CHRI has learned from sources who attended high-level policy meetings organized to address the implementation of the NIN that security and intelligence agents from the IRGC were not only regularly present, but served as the principal decision-makers at the meetings.[11]

One participant in the above–mentioned meeting told CHRI, "Agents from security agencies participate in most meetings with fake first and last names …they believe there is no way to control the internet, and that therefore we have no choice but to block the network's gateways inside and outside the country. This is the same policy pursued during the tenure of Mahmoud Ahmadinejad. Put simply, they want to launch an intranet."

In addition, the Intelligence Organization of the IRGC assumes a lead role in targeting individuals, organizations and websites for surveillance and cyberattacks. For example, they directed and led the "Spider" operation, aimed at monitoring and bringing down social media networks that facilitated western cultural "infiltration."

Rouhani's influence

Despite the more marginalized role of the president and his ministries, the implementation of internet policies, if not the policy making itself, remains in the hands of the Ministry of Communications, which is under the authority of Rouhani. Hence on several occasions, he has been able to directly intervene and prevent the implementation of policies with which he disagreed.

For example, on May 6, 2014, through a direct order to the Ministry of Communications, and in opposition to an earlier decision by the Working Group to Determine Instances of Criminal Content to block the messaging application WhatsApp, Rouhani successfully had the ban reversed.[12]

The Rouhani administration's efforts also led to the removal, in May 2014, of limits on internet speeds over 128 kbps. [13] Previously, nothing faster that 128 kbps had been allowed. These slower speeds had hampered Iranian civil society, rendering the internet largely useless for transferring the large files often used by activists and journalists.

Rouhani had long asserted the need to address the issue of internet speeds in the country. For example, In May 2014, Rouhani said at the Fourth Annual Festival of the ICT, "I, as president, am not happy with the bandwidth conditions in the country. We have reached an agreement with the Ministry of Communications and Information Technology to as soon as possible, to make third and fourth generations of broadband width available not only for homes and commercial centers, but also for cellular phone users, and to use the capacity of the private sector in the best way possible to this end."[14] Rouhani's lifting of these limits was framed within the context of the broader modernization of the country's information and communications technology infrastructure, but the benefits to internet access and use by civil society were significant.

"We ought to see [the internet] as an opportunity. We must recognize our citizens' right to connect to the World Wide Web."

President Hassan Rouhani, May 2014

Yet even in the areas of implementation, as opposed to policy, Rouhani has had to push to affect policy—receiving significant resistance along the way. On the bandwidth issue, for example, hardline critics of Rouhani argued that the issue is not within the president's jurisdiction. In a May 2014 article, the conservative paper Kayan wrote, "The Working Group to Determine Instances of Criminal Content is responsible for determining the issues and protecting the people's interests, which falls in the area of the judiciary's responsibilities and if [Rouhani's] statements are to be regarded as instructions, it would represent intervention in other branches' affairs and is in violation of Article 57 of the constitution."[15]

As bandwidth is well within the technical implementation role still afforded to the administration, the criticism illustrates the increasingly sharp struggle within the state for control over the internet in Iran. Indeed, the internet has emerged as one of the central battlegrounds within the state, both because of its importance in controlling the citizenry's access to information, and the divergent views between the Rouhani administration, which sees it as central to the modernization of the country, and hardliners, who see it as a threat to their control.

Ahead of Iran's February 2016 parliamentary elections, the Rouhani administration came under pressure by the Working Group to Determine Instances of Criminal Content and the Iranian judiciary to shut down the popular Telegram instant messaging application. The messaging app, now used by some 40 million Iranians and all political groupings in the country, was particularly important to groups promoting reformist, centrist and pro-Rouhani candidates, as these groups cannot use the state-controlled broadcasting and print outlets available to hardline groups and candidates. The administration was able to successfully oppose these attempts.

Rouhani's Minister of Communications Mahmoud Vaezi said on February 26, 2016, "We have had a lot of discussions at these meetings. Some agencies put a lot of pressure [on the council] to disrupt the internet in the run-up to the elections, or to block certain social media, but we opposed it."[16] The messaging app, now used by some 40 million Iranians and all political groupings in the country, was particularly

"Foreign cell phone messaging networks such as WhatsApp, Viber, and Telegram… [provide] grounds for widespread espionage by foreign states..."

Deputy Prosecutor for Cyberspace Affairs Abdolsamad Khorramabadi.

important to groups promoting reformist, centrist and pro-Rouhani candidates, as these groups cannot use the state-controlled broadcasting and print outlets available to hardline groups and candidates.[17]

Yet reflecting the constant tug of war over the blocking of such platforms, in April 2017, on the threshold of the country's presidential election, the Rouhani administration was unable to stop the blocking of Telegram's popular Voice Call feature ordered by the country's judiciary.[18]

More recently, during the unrest that broke out throughout Iran in late December 2017, the social media platform Instagram and the messaging app Telegram, widely used by the protesters, were quickly blocked, as were access to VPNs and other circumvention tools.

Since his first campaign for president in 2013, Rouhani has publicly supported greater internet access for Iranians. In May 2014, for example, he said, "We ought to see [the internet] as an opportunity. We must recognize our citizens' right to connect to the World Wide Web," as quoted by the official IRNA news agency. While seemingly tame, such remarks were delivered in a context in which supreme leader Khamenei was stating that the internet is "used by the enemy to target Islamic thinking,"[19] and officials such as Deputy Prosecutor for Cyberspace Affairs Abdolsamad Khorramabadi were saying, "Foreign cell phone messaging networks such as WhatsApp, Viber, and Telegram… [provide] grounds for widespread espionage by foreign states on the citizens' communications [and] have turned into a safe bed for cultural invasion and organized crime."[20]

Public expressions of support and isolated unblocking notwithstanding, Rouhani's overall record on internet access has not been impressive, and on internet security it has been extremely poor, as will be discussed in greater detail in the filtering and cyberattacks sections of this report.

During his first term (2013-2017), for example, at least 25 different tools that could provide users with secure online communication and browsing capabilities were blocked by the state. Over the past three years, access to secure messenger tools such as Signal[21] and Crypto.cat,[22] and the secure, privacy-friendly search engine Duckduckgo,[23] have also been filtered and made inaccessible to Iranian users. In addition, major social media platforms such as Twitter, Facebook and YouTube all remain officially blocked in Iran, and the Rouhani-appointed Minister of Communications Mahmoud Vaezi admitted that the Ministry of Communications had filtered "seven million" websites during Rouhani's first term.[24]

This picture shows that the request to open the DuckDuckGo search engine without an SSL certificate leads the users to the filtering page, therefore Iran has filtered this search engine.

Perhaps most significantly, Rouhani has also not sought to hinder development of the NIN, even though its development has enabled the state to more effectively filter online content, monitor and access users' online communications, and, critically, disrupt or cut off Iranians' access to the global internet—a capacity demonstrated for the first time on December 30, 2017 after widespread street protests broke out throughout Iran. In fact, development of the NIN has accelerated under Rouhani, and state policies promoted during his tenure have aggressively encouraged Iranian users to use the sites and services of the NIN, such as its national email and messaging applications developed to replace Telegram and other encrypted apps.

Rouhani has also kept silent during his tenure on illegal activities such as cyberattacks[25] against political and civil activists, journalists and even his own cabinet members.[26] Article 25 of the Iranian constitution states: "The inspection of letters and the failure to deliver them, the recording and disclosure of telephone conversations, the disclosure of telegraphic and telex communications, censorship, or the willful failure to transmit them, eavesdropping, and all forms of covert investigation are forbidden, except as provided by law."

Yet Rouhani, despite his promulgation of a Citizens' Rights Charter, has made little if any effort to protect the citizenry in cyberspace, or attempt to explicitly extend the legal framework to protect digital communications.[27] The NIN, which facilitates state access into accounts, and which, in all likelihood, will be used to facilitate the covert state surveillance of individuals, is a direct violation of citizens' rights.

In sum, Rouhani's record is decidedly mixed: his ability and/or willingness to extend political capital has varied considerably on internet issues. He has verbally defended internet freedom on numerous public occasions, unblocked some messaging apps on a few occasions, and upgraded Iran's ICT infrastructure to enable greater internet speed and use. Yet he has also allowed extensive filtering and social media blocking to continue, has overseen the accelerated development of the NIN, which, as discussed, has given the state the demonstrated capacity to cut Iranians off from the global internet (in addition to enhanced online surveillance capabilities), and, as will be discussed, has presided over a notable increase in state-sponsored cyberattacks without public comment. This, despite his pledge, as late as summer of 2017 during the announcement of his new cabinet members, that his administration would not filter the internet. Overall, Rouhani's actions have fallen well short of his rhetoric. He has not protected Iranians' right to access information or their right to online privacy, actions that have left the people of Iran vulnerable to internet disruptions and cut-offs and to state intelligence and security agencies that can access users' private online communications.


YouTube
Trending
History
BEST OF YOUTUBE
Music
Sports
Gaming
Movies
TV Shows
News
Live
Spotlight
360° Video
Browse channels

Iran's National Information Network

Background

Implementation Phases

Speed and Bandwidth

Services and Tools of the NIN

Background

Iran's National Information Network (NIN) has emerged as the central plank of the Islamic Republic's efforts to control its citizens' digital access and communications.

The initial concept was to create a state-controlled and censored version of the global internet, originally called the "National Internet," after which access by Iranian users to the global internet would be severed. Its purpose was to allow Iranians access only to state-approved content.

Yet officials realized that such an action was not technically feasible, as it would interrupt the activities of universities, banks, companies, government offices, police and many other organizations that would need to be connected to the global internet. Furthermore, even if it was possible to cut off Iranian users from the global internet and to issue special permits for certain organizations to be allowed access to it, it would be nearly impossible to administer and monitor their access.

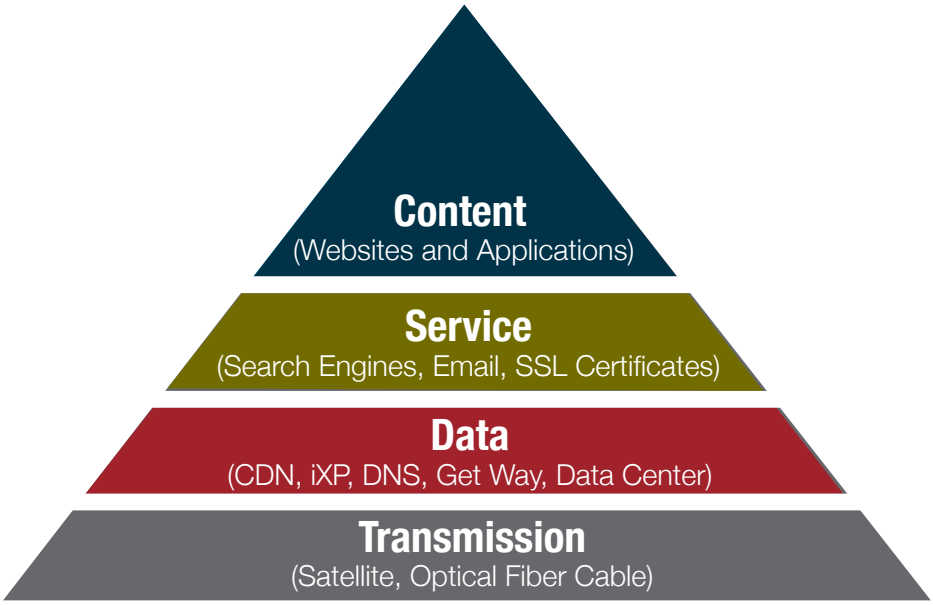
As a result, the concept was withdrawn; what Iranian officials had referred to as the "National Internet" or the "Halal Internet" became the "National Information Network."[28] This National Information Network (NIN) is a state-controlled network on which Iranian users are able to use domestic (state-issued) facilities such as search engines and email services, conduct bank and trade transactions, and access content produced inside Iran, without having to use international services. Access to the global internet is possible, but users inside Iran must now go through the NIN to access the global internet. Critically, the NIN has allowed the state to separate international from domestic internet traffic. This has given the government the ability to cut off Iranians' access to the global internet at will, while maintaining domestic access to the NIN—a capacity that was demonstrated, as previously mentioned, for the first time on December 30, 2017, when the government completely severed Iranians' access to the global internet for a half-hour after unrest broke out across the country.

Most of the increases in internet speeds have been used for internet connections for sites hosted inside the country.

Since 2014 and concurrent with Rouhani's presidency, phases 1 and 2 of the NIN have been launched. These phases have primarily concerned laying the technical groundwork for separating international from domestic internet traffic, keeping Iranian internet traffic inside the country, and providing the infrastructure for hosting content inside Iran.

The NIN is augmented by domestic services that mimic global online services (for example, a video service called Aparat, which is the NIN's version of YouTube) that drive traffic to the NIN because the government makes them faster and cheaper for Iranians to use than the corresponding global services.

The increase in internet speeds, while promoted by Rouhani as central to the digital modernization necessary for the country's economic and professional vitality,



COMPONENTS OF THE NIN

has also been integral to the success of the NIN. A little publicized aspect of the bandwidth increases has been the extent to which most of it has been funneled into the domestic connections used by the NIN. While internet speeds have improved across the board for both international and domestic internet traffic, and this has brought significant benefits for internet use throughout the country, the lion's share of the increases has been used for faster internet connections for sites hosted inside the country.

The NIN has been sold to the Iranian public on the basis of government claims that it is cheaper, faster and more secure than the global internet. As will be detailed in this report, these claims are problematic and do not take into account the losses to Iranian users in uncensored access and online privacy.

While the cost of internet access has indeed been reduced and speeds have increased significantly, the NIN has also allowed state censorship to be implemented on a wider and more sophisticated scale, strengthened the state's online surveillance capabilities, and enabled the state to disrupt or cut off Iranians' access to the global internet. While it is yet to be determined if the NIN will provide its users with greater technical security from some types of hackers and digital threats, the NIN will make it easier for state security, intelligence, and judicial agencies to monitor, hack and disrupt citizens' online communications.

Implementation Phases

The NIN has been developed in three phases, two of which were launched during Rouhani's first term. Mohammad Javad Azari Jahromi, then deputy minister of communications, stated on February 7, 2017, that the third phase was to begin on May 17, 2017,[29] International Telecommunications Day. However on April 3, 2017, then Minister of Communications Mahmoud Vaezi informed the Mehr News Agency of a delay in the launch. "Considering the upcoming elections in the country, the third and final phase of the National Information Network will be launched after the elections," he told Mehr."[30]

Iranian officials have defined the goals of the first two phases of the NIN as follows:[31]

First Phase:

> Access to E-Government[32] services, video services inside the country and a variety of online financial services.

> Offer bandwidth and higher speeds for land and mobile lines, and access to content and services inside the country.

> Increase network quality (i.e. the reduction of disruptions).

> Reduce final price of an internet connection for consumers.

Second Phase:

> Increase the number of internal data exchange traffic centers (iXP) from four to seven.

> Increase Iran's data transfer network from four terabits per second to 10 per second.

> Launch a "data mining" system to monitor viruses in the network.[33]

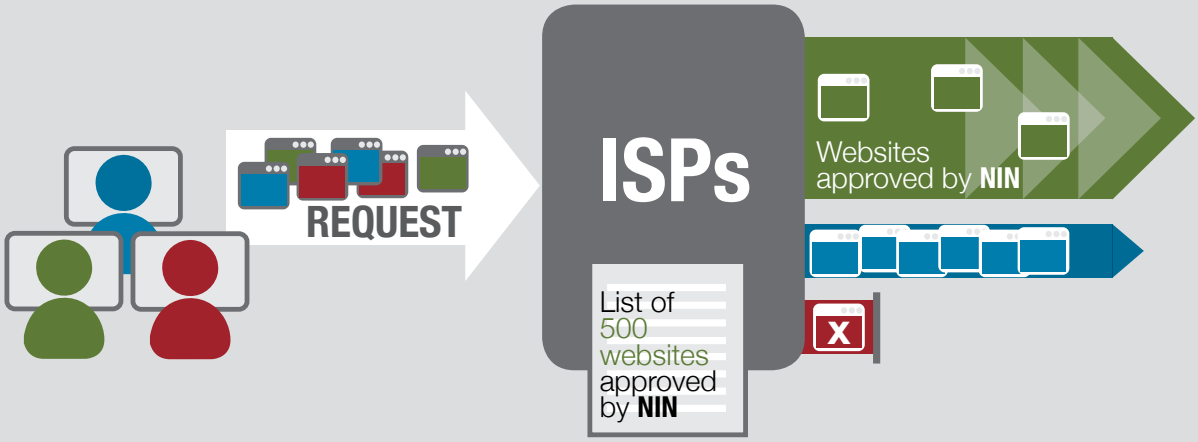
> Increase the average internet access speed in third generation mobile phones (3G) to approximately 2MB; in the fourth generation of mobile phones (4G) to approximately 12 MB per second; and in ADSL networks to approximately 5 MB per second.

> Require all providers of fixed and mobile internet to separate their rates for domestic and international rates. The rates for domestic traffic will be calculated at 50% of the international traffic bandwidth.

These goals are discussed in more detail in the following sections.

Speed and Bandwidth

One of the main objectives of the first and second phases of the NIN was to increase bandwidth in Iran. Until recently, internet service providers were not allowed to



NET NEUTRALITY ISSUES WITH THE NIN

Three results can occur if a person tries to access a website while using NIN. If the website is filtered, the user will be denied access and directed to a filtered website notice page. If the website has been approved by NIN, the user will be able to access it at a discounted rate and at a faster loading speed. If the website is not filtered, but is not included on NIN's "approved" list, the user will gain access at the regular speed and price.

offer speeds faster than 128 kbps to home users. The removal of this constraint, advocated by and achieved under the Rouhani government, has enabled providers to offer services at higher speeds.

Undertaken simultaneously with this has been the segregation of internal and external network traffic. This segregation means that if users request access to content within the country and within the NIN, they will be able to use the faster (domestic) path, as opposed to the one they would have to use to access content outside the country. This has enabled the government to not only offer higher speeds for domestic traffic but also lower costs.

Mohammad Ali Yousefizadeh, the managing director of Asiatech Company, one of the largest internet service providers in Iran, told Mehr News Agency on March 11, 2017, "Currently, more than 200 internal websites with the highest traffic are accessible at half the price of international internet access."[34] This number has now increased to 500 domestic websites.

For example, the Asiatech[35], Rightel[36], and IranCell[37] companies signed an agreement[38] with the Communications Infrastructure Company[39] whereby users who visit national websites such as Aparat[40], Filimo[41], Telewebion[42], and RazavaTV[43] (which provide live broadcasts of the Shrine of Imam Reza in Mashad), will pay access rates that are 50% to 100% lower than their normal rates.

When users access websites outside the country however, the access rates have not been similarly reduced. Faster speeds and lower costs for domestic content are central to the state strategy to steer user traffic to the NIN.

By favoring domestic traffic, Iran violates the principles of net neutrality, According to the Global Net Neutrality Coalition, "To guarantee freedom of choice and information, net neutrality promotes the idea that internet traffic shall be treated equally, without discrimination, restriction or interference regardless of its sender, recipient, type or content, so that internet users' freedom of choice is not restricted by favoring or disfavoring the transmission of internet traffic associated with particular content, services, applications, or devices."[44]

The Iranian government is violating net neutrality by segregating the internet into global and domestic networks for the purpose of offering higher speeds and lower rates for those who access domestic content. Disregarding net neutrality could potentially lead to the violation of the rights of online users and endanger their privacy because it enables the state to monitor private traffic and determine what sites users are accessing. Monitoring traffic should only be carried out under the law.

Iran's Cyber Crimes Law makes several references regarding access to user traffic, and it prohibits eavesdropping. Articles 1, 2 and 3 ban "unauthorized" access or surveillance of online data. Violations carry a punishment of one to three years in prison or a fine. However, the law does not define authorized access.

In the US, federal laws restrict network monitoring to "headers" information, which only describes IP version, total Length of IP packet, source and destination address and other non-sensitive information. In his June 2017 statement, UN Special Rapporteur on the Right to Freedom of Opinion and Expression David Kaye said repressive governments "are shutting down - or demanding that third parties shut down - services, including in times of public protest and mass dissent. Many are demanding that service providers retain and share user data. Still others are rolling back much-needed protections for net neutrality."[45]

Iran's second largest mobile network service provider, Irancell (MTN), admitted on May 1, 2017, that VPN users won't qualify for the 50 percent discount on monthly internet costs offered to those who limit their usage to 500 sites on the NIN. Other mobile and web service companies have followed suit. Offering these discounts to discourage Iranians from accessing banned sites fundamentally violates net neutrality, which requires that "a maximally useful public information network aspires to treat all content, sites, and platforms equally."

The objectives of the second phase of the NIN are to provide the average internet access speed of approximately 2 Mbps in third generation mobile telephones (3G), approximately 12 Mbps in fourth generation (4G), and approximately 5 Mbps in household DSL networks.[46]

According to a report by M-Lab website, which collects and analyzes more than 200 million tests of internet speeds worldwide, between 2013 and 2017, Iran's internet speed for international traffic escalated from 0.3 Mbps to approximately 1 Mbps.[47]

Although Iran's international internet bandwidth has more than tripled over the past four years, this improvement is still less than the average internet bandwidth compared to countries in the region such as Turkey, with 3 Mbps, and the UAE, with 3.5 Mbps. The table below compares the bandwidth of Iran's 12 neighboring countries based on M-Lab website reports:

Ranking	Country	Average Speed (Mbps)
1	Qatar	5
2	Oman	4.2
3	The United Arab Emirates	3.5
4	Turkey	3
5	Bahrain	2.6
6	Kuwait	2
7	Azerbaijan	1.8
8	Armenia	1.8
9	Saudi Arabia	1.6
10	Iran	1
11	Pakistan	0.7
12	Iraq	0.7
13	Afghanistan	0.7

Source: M-Lab, www.measurementlab.net

For mobile phones, internet speeds have also significantly improved. Mobile phones are increasingly central to Iranian online use: According to the Mehr News Agency, as of June 20, 2016, about 22 million Iranians use mobile internet—far more than home internet users.[48] (ADSL internet users in the same period were nine million.) Between 2013 and 2017, the average internet speed for mobile phones increased from 0.2 to 2.4 Mbps due to the availability of 3G and 4G mobile services.

Additionally, during the same period, the Rouhani administration ended the Rightel Company's monopoly over 3G and 4G mobile services, enabling other mobile phone service companies to offer these services to their users.[49] Nevertheless, mobile users still face the same environment as that of home users, with faster speeds and lower prices steering users to state-controlled domestic sites.

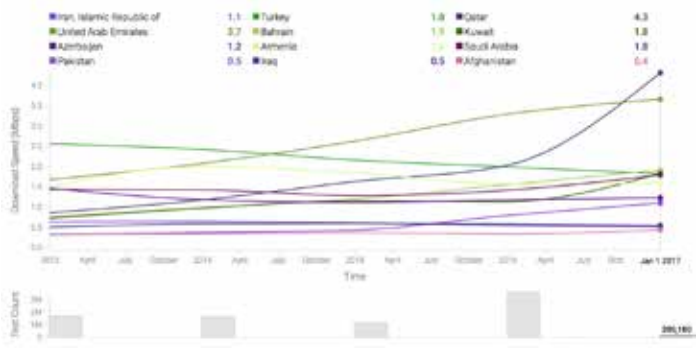


Chart shows internet speed and bandwidth changes since the beginning of 2013 through July 1, 2017 in 12 neighboring countries of Iran, based on data from M-Lab's website.

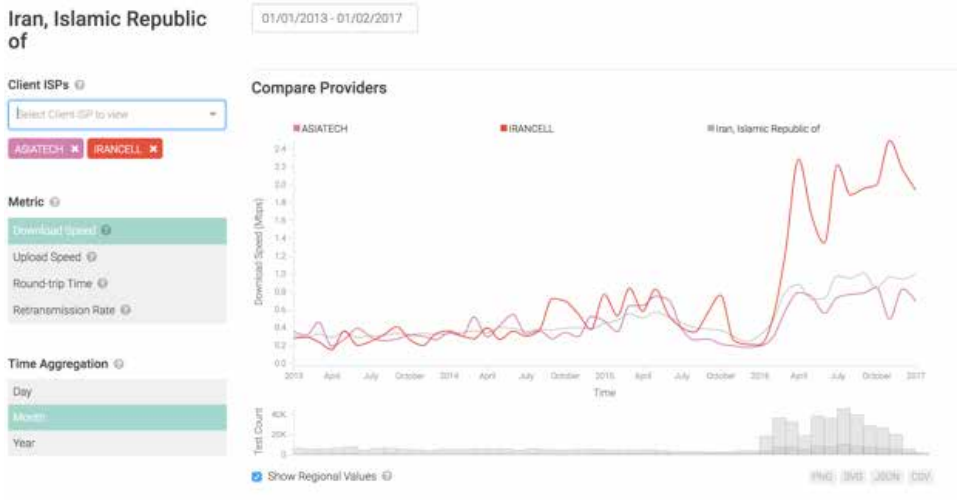


Chart compares internet speed provided by Asiatech Company (household internet) and Irancel (mobile internet) between 2013 and 2017, focusing on international internet traffic. Source: M-Lab website

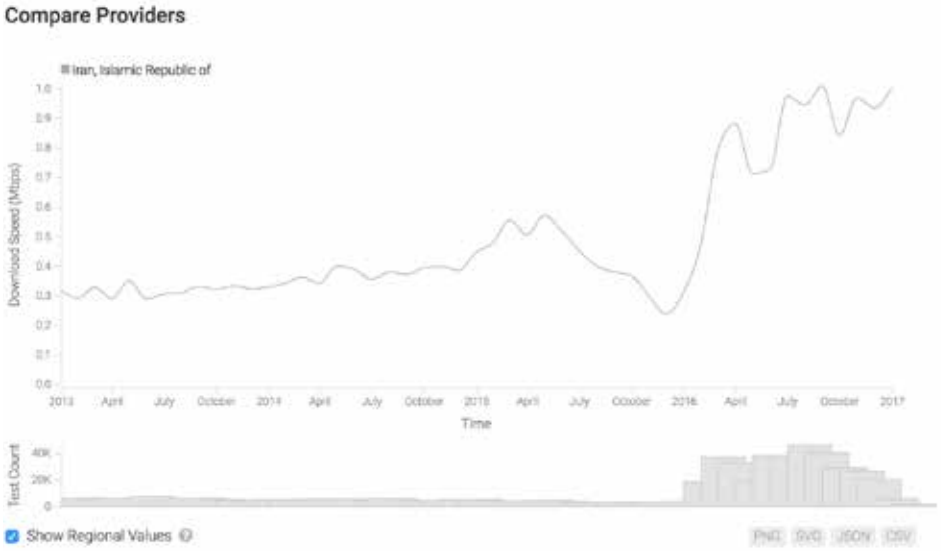
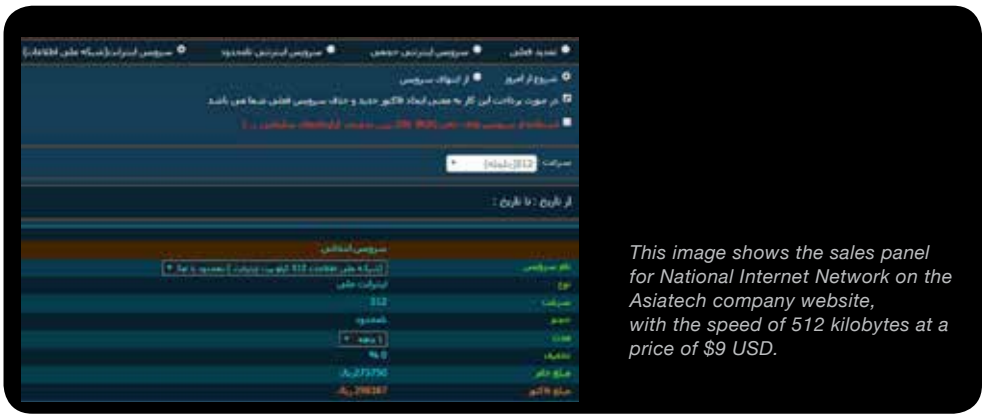


Chart compares average speed and internet bandwidth changes for 20 internet service providers in Iran between 2013 and 2017, focusing on international internet traffic. Source: M-Lab website

The opening of content delivery and data exchange centers during Rouhani's first term has played an important role in the increased internet speed. The Internet Exchange Point (IXP) is a physical infrastructure responsible for reducing the data traffic being transferred between content delivery networks and internet service providers. The advantage to using the Internet Exchange Point is its role in reducing the traffic between content delivery networks and ISP's. The reduction of data transfer costs and the increase in the bandwidth are among the results of the utilization of these centers.

Currently seven[50] Internet Exchange Points (IXP) have been launched by the Communication Infrastructure Company, a government entity affiliated with the Ministry of Communication and Information Technology, in the cities of Tehran[51], Qom[52], Mashad[53], Shiraz[54], Tabriz[55], Isfahan and Ahvaz.



This image shows the sales panel for National Internet Network on the Asiatech company website, with the speed of 512 kilobytes at a price of $9 USD.

Implications

The increase in speed has had important implications that has affected all aspects of Iranian society—political, social, business, academic and cultural. It allows the transfer of large files, video streaming, the use of VoIP (Voice over Internet Protocol, used in messaging applications such as WhatsApp, Telegram and Signal), video conferencing and other services that greatly increase and improve access and more sophisticated information sharing. This has not only facilitated general communication amongst the public, it has been critical to the work of journalists and activists in Iran. Greater internet speeds have also enhanced professional, academic and commercial communications, as well as the ability to develop Iranian start-ups and online services. However, it should be noted that the higher speeds are still vulnerable to state action, as demonstrated by the government's decision to significantly slow down the internet, in an effort to disrupt traffic to the global internet, during the initial days of the unrest in late December 2017.

Network Access

The user must go through the NIN to access information on the global internet.

From the first day of the formal launch of the NIN on August 28, 2016, all Iranian users' traffic has occurred, by default and without choice, within this network. In this environment, the user is not disconnected from the global internet, but he or she must go through the NIN and use the NIN to access information on the global internet. This means the Iranian government has the ability to connect—or disconnect—all users in Iran from the global internet. This capacity was demonstrated for the first time on December 30, 2017, when the government, after imposing significant internet slowdowns, severed Iranians' access to the global internet for a half-hour.

The internet service provider (ISP) is responsible for separating the users' traffic into internal (domestic) and external (international) traffic, and must show the user on a monthly basis what portion of his or her internet usage was on the internal network and what portion was on the global internet, and the corresponding costs. In most countries, ISPs are private companies which set their own prices, but in Iran the government sets all of the prices through the state-run Infrastructure Company—and it sets the domestic price lower than it sets the international price, thereby steering traffic to the NIN.

Some of the ISPs in Iran also offer users a choice of purchasing access only to the NIN—an option that means the user will only see content available on the state-controlled network. In this situation, users have no access to content outside of the NIN. For example, on this plan, a search for the New York Times' website would not render any results. This option is again encouraged by the government through its cheaper pricing—and the faster speeds available for domestic connections.

Asiatech, one of the first ISP companies to offer access to the NIN as a separate service, offers the service at 128 Kbps and without download limitations at the equivalent of $3.67 USD per month, while the price for the same access to the global internet is $7.70 USD per month. Asiatech was the first company to update the order page on its website with the notice to its users that by choosing this type of (domestic only) connection in Iran, they would not have access to websites on the global internet. The company does not set or even have any say in the pricing, rather, it is set by the government. Through these price incentives, the state discourages traffic away from the global internet, and toward state-approved content.

A computer network specialist in Iran spoke with CHRI about this service option: "If you purchase [this NIN-only connection], accessing anything outside Iran is impossible and the user will only be able to use the network within Iran. For example, with this service, if you try to open www.google.com, you will receive a message that the network is not able to find this website."

This image shows the sales panel for the NIN on Asiatech's website. The text in red warns: "Dear Subscriber, please be aware that by choosing this service, you will only have access to internal websites and you will not be able to access the Internet and websites outside the country."

Network Security

Iranian authorities and designers of the NIN have cited improved security as one of the most important benefits of this network, and that is prominently used to justify its development to Iranian users. According to their statements, the NIN will protect government organizations and agencies, as well as users, against cyberattacks and guarantee their security.

In September 2016, Esmaeil Radkani, the deputy director for ICT at the Communications Infrastructure Company said that the security of the NIN is "guaranteed" through the use of "DDos Protection" and "Anti-Phishing Protection" tools.

The ability of the NIN to protect users from DDoS or phishing attacks is, as of yet, undetermined. Yet the real issue for the NIN is the inherent lack of security for users against state security and intelligence agencies. These agencies have complete access to government resources for monitoring and identifying NIN users and their activities, and they do not need any legal authorization from state or judicial authorities to access users' accounts.

The issue for the NIN is the lack of security for users against state security and intelligence agencies.

User Security

Protecting the privacy of their online communications is one of the main concerns of Iranian users. For over a decade, human rights defenders, activists, ethnic and religious minority rights leaders, students and journalists have been routinely targeted for hacking attacks by Iran's security and intelligence organizations, especially Iran's Islamic Revolutionary Guard Corps (IRGC).

Such attacks have never been followed by any explanations by Iran's internet authorities or Iran's Cyber Police (FATA)—even when such hacking attacks were against (reformist and centrist) state officials, and, more recently, members of President Rouhani's own cabinet such as former Vice President for Women and Family Affairs Shahindokht Mowlaverdi.[56]

Iranian authorities have never taken any effective steps, whether by legislative or judicial means, to protect user security and privacy, despite the fact that they are obligated to do so under international covenants it has signed such as the International Covenant on Civil and Political Rights (ICCPR) and under Article 25 of the Iranian constitution which forbids unlawful eavesdropping.[57]

With the development of the NIN by Iranian state organizations, which can provide the country's intelligence and judicial organizations with full access to online communications for domestic applications/services, the concern is greater than ever. In an environment where regulatory and judicial oversight limiting state access to citizens' online communications are not present, state-sponsored surveillance and hacking of online communications presents users with profound risks.

User Authentication

As the NIN has become operational under the Rouhani administration, significant new state capabilities have been developed that facilitate state access to users' accounts.

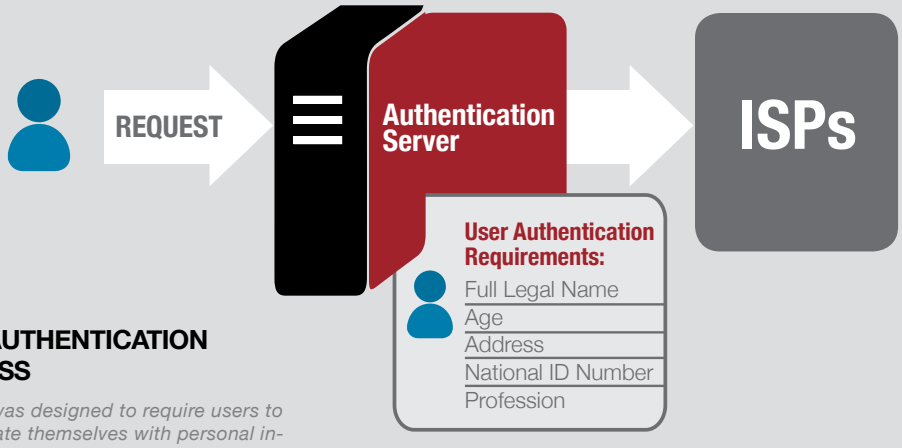
For example, the requirement for all users in Iran to have a single, unique identifier for accessing the internet, which is planned for the third and last phase of the NIN (expected to be undertaken during Rouhani's second term, 2017-2021), will significantly compromise user privacy. Nasrollah Jahangard, deputy minister of communications, said at the opening of the first phase of the NIN that user authentication will be a requirement in this network, adding: "All connections, whether fixed or mobile (phone), will have a single identity, and if the user lacks the identification, it will not be possible to provide him/her with service."[58]

While this authentication process does not yet exist, after this phase is launched, all users will have to enter the network with their National Identification Number, making their activities identifiable. Because their online activities will be saved, if intelligence and judicial authorities wish, they can access a log of their activities.

Jahangard denied this, saying, "Authentication of users does not mean that we are monitoring the data exchanged by them."[59] Yet his claim is not accurate; NIN access via National Identification Numbers will allow Iranian authorities to monitor the online activities and the information exchanges of users.

Servers and websites hosted inside Iran

A second central security concern is the intention to transfer all servers and the hosting of Iranian websites to Iran—a move explicitly stated as one of the main objectives of the NIN.



USER AUTHENTICATION PROCESS

The NIN was designed to require users to authenticate themselves with personal information before accessing content. This process has yet to be implemented.

Jahangard told Jahan Eghtesad Newspaper that the reason for the transfer is to reduce internet costs: "From an economics point of view, transferring this volume of data traffic into the country, as well as hosting the websites inside the country, will lead to a reduction of the cost of the transferred network, and for example, the user can receive a movie or a file faster, with higher quality, and at a cheaper price."[60]

It is true that these conditions will deliver faster and cheaper online access to Iranian users. It will also severely degrade user security: placing servers inside Iran or hosting Iranian websites inside Iran allows state access to the content of those websites and their user accounts.

For example, if instead of using Gmail an individual uses the Iranian email package Chapar, because Chapar stores data from its users inside Iran, whenever security officials wish, they can receive the entire content of that individual's emails.[61]

Similarly, if news websites or blogs are hosted inside Iran, when they post articles disapproved of by the authorities they can be shut down and their entire data can be deleted by the state. After the Memari News website published documents about corruption at the Tehran Municipality, the secretariat of the committee to determine instances of crime ordered the managing director of the Shatel Company, which hosted the Memari News website, to delete all of the website's content from the internet.[62]

In March 2015, at a meeting to evaluate the issues and challenges facing OTT[63] and domestic social media, then Minister Mahmoud Vaezi confirmed the issue and stated that managers of these companies have privately told him, "Many Iranians prefer to have their servers managed abroad to ensure that in case of filtering, they would not lose data belonging to their foreign customers."[64]

"Many Iranians prefer to have their servers managed abroad to ensure that in case of filtering, they would not lose data belonging to their foreign customers."

Rouhani's former Minister of Communications Mahmoud Vaezi, March 2015

SSL security certificates

The privacy and security of Iranian users has also been eroded through the use of Iranian national SSL security certificates. While SSL security certificates ensure the security of the connection between the user and the websites by encrypting the internet traffic, this security is built on trust in the provider of the security.

Any entity issuing a SSL certificate has two "keys" for that certificate—one for encrypting and one for decrypting.

While a company will keep those keys secure, if the state is the issuing body, they also have the ability to decrypt—without the worry of going out of business. Given the Iranian government's history and record of violations of users' privacy, trust in the integrity of the certificates would be misplaced. Because they are state-issued, Iran's national SSL certificates offer only a false security—regardless of the "https" users will see in the address bar. At present, the Iranian national SSL certificate is valid only in Iran and in Iran's Saina[65] national browser; no other browser currently regards it as valid.

According to Article 32 of Iran's Regulations of Electronic Commerce Law,[66] the (state-run) Center for Root Certificate Authority (CA)[67] is responsible for the authorization to create, sign, issue and revoke the national SSL certificates. The Iranian government will thus control the issuance, use and distribution of the national SSL certificates. Simply put, use of this security certificate–by individuals, websites or mobile applications—will enable state intelligence and security forces to access, surveil, hack and control users' internet content.

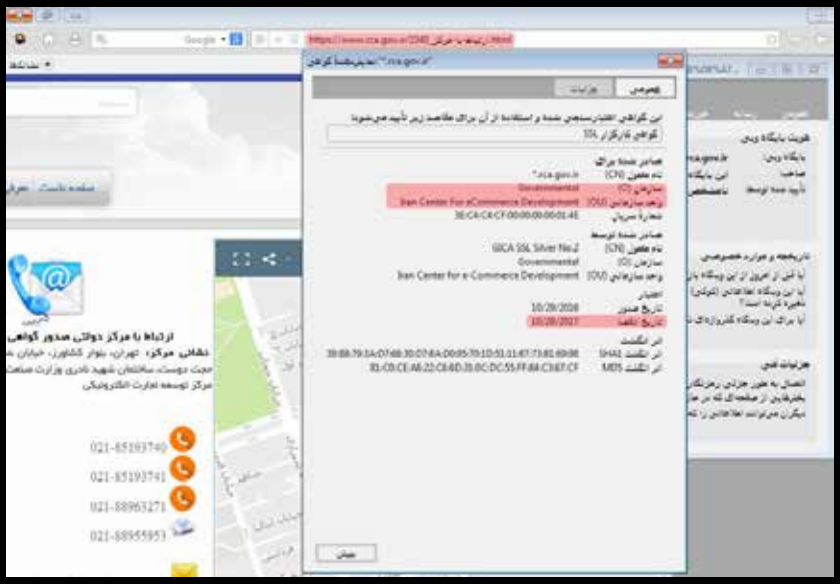
So far, the Iranian government does not appear to have made much headway with its SSL certificates. The last available numbers published on its website[68] are from March 2014, and indicate 440,000 copies of Iran's national Saina browser were downloaded. While the data is several years old, the fact that Iran's national SSLs are still not recognized as valid by any other browser suggests these numbers have not moved significantly. Nevertheless, If Iran is successful in pushing more users to use them, Iranians' online privacy will be deeply compromised.

Implications

Creating ID's for all Iranian users, hosting Iranian websites in the country, and using Iran's national SSL certificates, taken together will enable state agencies to access Iranians' online communications. As such, they will leave Iranians defenseless against Iran's intelligence and security agencies, which continue to use their capabilities in cyberspace to monitor online activity, identify perceived opponents, and, in collaboration with Iran's judiciary, prosecute political and civil activists on the "evidence" of online content with which they disagree.

Services and Tools of the NIN

Developing the NIN as an alternative to the global internet has necessitated the development of many auxiliary tools, services and other aspects of technological infrastructure. Over the course of the last 10 years, the Iranian government has made progress, even if uneven, toward this aim. Following is a discussion of some of the key aspects of that development.



This image shows validity of the national certificate on the website of the Center for Root Center Authority (CA), which has been opened with the Saina national browser.

```
; This file is not used. If you modify it and want the application to use
; your modifications, start with the "-app /path/to/application.ini"
; argument.
[App]
Vendor=MATMA
Name=Saina
Version=2.0.1
BuildID=20160129065234
ID={ec8030f7-c20a-464f-9b0e-13a3a9e97384}

[Gecko]
MinVersion=1.0.20
MaxVersion=1.0.20

[XRE]
EnableProfileMigrator=1
EnableExtensionManager=1

[Crash Reporter]
ServerURL=https://crash-reports.mozilla.com/submit?id={ec8030f7-c20a-464f-9b0e-13a3a9e97384}
    &version=2.0.1&buildid=20160129065234
```

Image exhibits the configuration file of Saina browser, which shows Mozilla servers are still used for error reports

National Electronic Mail Services

During the Ahmadinejad government (2005-2013), three national email services, Chapar, Iran Post Company, and Iran Dot IR were launched in Iran.[69] While all three of these email services are still operational, during Rouhani's administration (2013-present), Iran Dot IR has become the main national email service and has been integrated into the government's "Electronic Dashboard System," a national portal where Iranians can access government services (including email), communicate with government agencies, and access state and national information."[70]

Announcing the news in November 2015, Reza Bagheri Asl, vice president of the Information Technology Organization of Iran said, "Currently we are launching the 'Electronic Dashboard System,' and the Iranian government's national portal, in an effort to replace communications through email." The system provides national email services through mail.iran.ir, which is controlled and monitored by the Ministry of Communications and Information Technology.[71]

The Chapar email service remains active, although now it lists itself as a private company. The state-run Iran Post Company email service is also still available, but is no longer promoted by the government as the main national email service.

The boundaries between the services are blurred. For example, the Iran Dot IR email uses Chapar email software, as Chapar codes can be seen on both the server side and the client side of Iran Dot IR. In some cases, even public addresses on both sites are exactly the same. For example, the link to change user passwords on both email services is www.domain/Chmail/repassword. In another example, Iran Dot IR email uses Chapar's public key. This means Chapar has access to the content exchanged on Iran Dot IR.

The national email services store account information in Iran on the NIN where the state can read the emails.

CHRI's analysis of the SSL security certificates of both Chapar and Iran Dot IR provide another example of the questionable claim by the Iranian government that the NIN provides its users with superior security. For incoming emails, both services lack PFS Service, which adds a level of security to encryption.[72] If encryption keys are stolen, PFS makes decoding the previous data impossible. But for outgoing emails, an invalid certificate has been used, which means the outgoing emails are not encrypted, resulting in the possibility of tapping the traffic of transmitted emails.

According to CHRI's investigation and technical evaluation, as of March 2017, both Chapar and Iran Dot IR email services have also been using an outdated version of email server and client software. Failure to use updated versions of software applications leaves the door open for hackers to carry out cyberattacks. In June 2016, hackers (from outside Iran) were able to hack[73] several Iranian government websites, such as the Statistical Center of Iran, due to a security hole in an old version of DNN[74] software, a program similar to WordPress used for designing and managing websites by Iranian government organizations and agencies.

The national email services store account information and content inside Iran on the state-controlled NIN. This means that the state, which has access to the NIN's storage centers, can access and read the emails. To be sure, users can individually encrypt their content, but in general few people in any country context are familiar with email content encryption, as it is a technically complicated and cumbersome process for the average person. Without content encryption undertaken on the individual level, emails via the national email services in Iran are completely accessible to the state, without any judicial review or approval needed.

Data Centers

National data centers comprise an important part of the infrastructure of the NIN. These centers are responsible for data storage, maintenance and processing, and maintaining the space for hosting websites in the country, online email communications, domestic messaging services and all communications between government and non-government organizations and users inside Iran.

The data centers were privatized under the Rouhani administration,[75] but again, the term private sector is imprecise in the Iranian context, including in the technology sector. Most ostensibly private companies are either at least partly state-owned or owned by parastatal parent organizations. Iranian officials have stated that foreign companies have expressed interest in participating in launching the data centers. Communications Minister Mahmoud Vaezi told Fars News Agency in February 2015, "In the post-sanctions negotiations, the Chinese company Huawei asked to build data centers in our country and Iran agreed with the request."[76]

The ownership and state affiliation of the Iranian companies connected with these data centers is unknown. This lack of transparency raises security concerns because it means the nature of the state's continued involvement, if not control, is not known. Data centers play a central role in the maintenance of data for web hosting, email, and cloud processing, and are responsible for storing and protecting users' online information and communications. Given the record of online surveillance and hacking by Iran's security and intelligence organizations, any potential state involvement in or access to these data centers raises troubling security issues. Indeed, the aforementioned case in which state officials ordered a hosting company to delete the Memari News website's content after it reported on corruption in the Tehran municipality bodes poorly for the security implications of these data centers.

The ownership of the companies connected to Iran's national data centers is unknown; this means the nature of the state's involvement is unknown.

National Search Engines

Iran's national search engines are one of the government's main levers of control over information access across the NIN. These search engines determine the flow and presentation of content on the NIN, and, as such, internet censorship and content filtering is to a significant degree carried out at the search engine level on the NIN. Indeed, national search engines are considered the main axis of censorship in Iran.

Iran's national search engines block content and deliver fabricated information to the user.

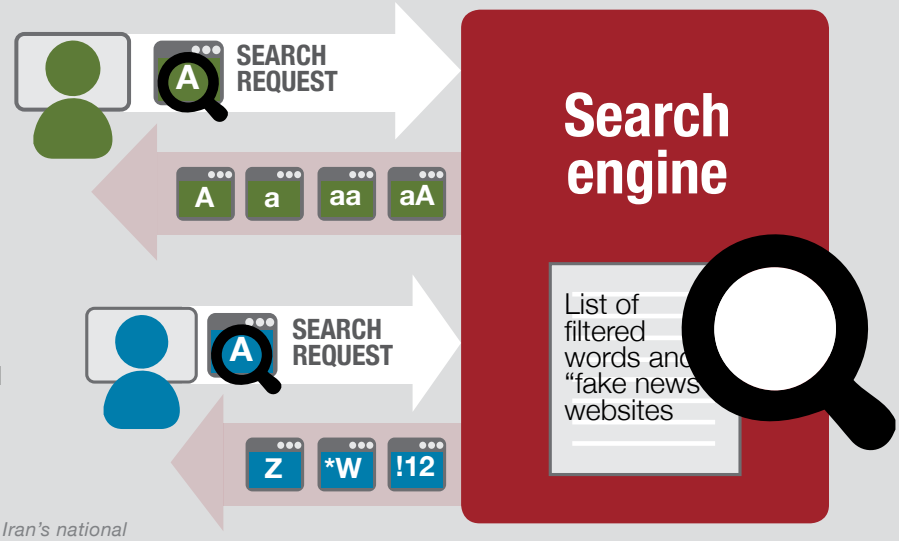
Prior to their emergence, one of the common methods used for filtering content in Iran was blocking based on key words. State agencies responsible for internet censorship prepared a list of words and sent them to the Communications Infrastructure Company. The software used for filtering would block the user's intended content when it identified one or more of these words. Since the launch of the NIN, national search engines have become responsible for this task.

Upon detecting any words or phrases that appear on the list of keywords, these national search engines either block the content or deliver fabricated information to the user, without issuing any message that would indicate the censorship or blocking of the content.

Censorship in Iran via the blocking of key words is not limited to the national search engines—the authorities also censor global search engines used inside Iran such as Google. Yet because these global search engines use international SSL security certificates that encrypt the traffic between the site and the users, Iran's filtering system is unable to "read" these key words and thus unable to impose its censorship. If the site is not using an international SSL security certificate, the user will face a filtering page.

For example, if a user in Iran types "facebook.com" on the Google search engine without using an SSL security certificate, he or she will face the filtering page. If the user types the same words in the Parsijoo national search engine, he or she will be shown fake information and websites, or in some cases, instead of showing the user the filtering page, a message stating "Search Unsuccessful" will be shown and the user is asked to narrow the search.

This image shows that without an SSL security certificate, the search results of news websites, social networks, and Google Play will direct the user to a filtering page.



HOW THE NIN'S SEARCH ENGINES REDIRECT USERS TO "FAKE NEWS" WEBSITES

With the development of the NIN, Iran's national search engines now automatically block key words and phrases—and send users to sites that deliver only state-approved and sometimes fabricated content.

Because of the difficulty in censoring international search engines that use encrypted web traffic, the Iranian authorities have intensified their promotion of the NIN and all its various auxiliary tools and services such as the national search engines. Iranians are bombarded continuously with advertising on state-run media that aggressively broadcasts the NIN's pricing incentives, increased speed, and (supposed) safety benefits.

The reception in Iran nevertheless seems to remain less than robust. On March 2, 2015, Farhad Elyashi, a member of the Tehran Computer Trade Organization's Software Commission said Iranian users will show no interest in using the national search engines. "There is this image that Iranian [search] engines present content in a filtered fashion, leading to [search] results that the user does not want and this is one of the reasons the Iranian search engines are not received enthusiastically," Mr. Elyashi told Khabar Online, adding, "A search engine that presents only partial results will not be received well."[77]

The authorities appear to be intensifying the censorship attributes of the NIN. For example, Iran's national search engines offer the user an option of "Intranet (NIN) Active/Inactive." Previously, this gave the user a choice between conducting the search on the NIN ("Intranet Active") or on the global internet ("Inactive"). If a user chose active, and searched for the website of reformist former Iranian President "Mohammad Khatami, who is now reviled by the Iranian government, the first result shown was a phony website linking Khatami to anti-US propaganda ("Mohammad Khatami's election website in the US"). The former president's website was not displayed in subsequent search results, either. If the same phrase was entered on the Google Search engine, the first result would be Khatami's actual website. Yet as of October 2017, the choice is no longer offered; selecting either Active or Inactive produced the same search result for Khatami: the bogus website.

The national search engines provide a world parallel to the real world in which only information in support of the state narrative of events is delivered.

Ministry of Communications and Information Technology officials have consistently denied the specific state filtering and deletion of content related to human rights or sensitive political issues. Nasrollah Jahangard, deputy minister of CIT told ISNA on February 24, 2016, "The politicized atmosphere has led us to consistently accuse Iranian software programs of … filtering."[78]

Yet CHRI research does not support Nasrollah Jahangard's comments. Searching for the names of civil activists or political prisoners, or topics such as the disputed 2009 presidential election, the serial killings of dissidents abroad during the 1990s, the mass executions of prisoners in the 1980's, or the financial corruption of current state officials, will all confirm that blocked information and state censorship remains robust in Iran. In effect, the national search engine provides a world parallel to the real world for Iranian users, in which only hand-picked information in support of the state narrative of events and individuals is delivered.

This image shows that Parsijoo search engine, which has been introduced as the "National Search Engine," provides forged and false information to the users.

Iran has also tried to encourage international companies that provide search engines to implement Iran's censorship policies in their search engine results. Alireza Yari, secretariat of the Steering Council of National Search Engines, said in September 2012 that they had sent letters to Google, but had not received a response from the company.[79]

In a state visit to Russia in November 2015, Mahmoud Vaezi, then Minister of Communications, announced[80] that according to an agreement signed with Russia, the developers of the Russian search engine Yandex[81] would soon open an office in Iran. At the time of the announcement, access to the Yandex search engine was blocked in Iran and as of April 2017, no changes have been made in this area.

The Iranian government has spent large sums on the devlopment of its national search engines. The failure of a number of them has not deterred continued investment, reflecting their perceived importance to the state's censorship efforts. For example, Gorgor, a search engine introduced as the national search engine in 2015, is no longer active and no official has ever offered any explanations for its quiet disappearance despite the resources that were allocated.

The model used to guide user search results on the NIN is one of the costliest and most sophisticated applications of its kind and the implementation of this policy by government ministries is in stark contrast to numerous public statements made by President Rouhani defending the right to access information. In fact, during Rouhani's presidency, the ability to manipulate the way content is presented in search results in order to achieve engineered results, a long-standing dream of opponents of free access to information, has become a reality.

The Iranian government's success in encouraging people to use the NIN will mean that in many areas—political, business, cultural, economic, scientific, social and even entertainment—Iranian users will be presented with filtered content, propaganda and intentional falsification by Iranian intelligence and security organizations, rather than real information.

On the NIN, Iranian users are presented with filtered content, propaganda and intentional falsification by Iranian security organizations.

Prior to the launch of the NIN, the state-run Islamic Republic of Iran Broadcasting organization (IRIB) was bestowed with this responsibility. Yet during the past decade, the IRIB has lost influence, credibility and power, as satellite television networks based outside Iran and the internet have broken its monopoly on information. In his letter appointing Abdolali Asgari as the new head of the IRIB, Supreme Leader Ali Khamenei advised him to have "an effective presence in cyberspace," reflecting the importance of the internet to Iran's highest official.[82]

National Operating System

One of the proposed elements of the infrastructure of the NIN is the National Operating System (NOS). Iran's national SSL certificates are built into the NOS and the National Browser. Yet six years after Iran's Communications Ministry published their "National Operation System Report" detailing the plans and goals of the system, and more than five years after its first version was introduced in 2010, the operating system remains unavailable to users, without public explanation.[83]

At a press conference at the 16th Tehran International Telecom Expo in September 2015, Deputy Minister of Communications Nasrollah Jahangard announced that the NOS would be launched in October 2016, and that its operational phase would begin soon, "after some applications are installed on this Operating System,"[84] yet since then no version of this OS has been made available to users, again, without comment or explanation.

Cyber Attacks

Tactics and Methods

Implications

During Rouhani's first term (2013- 2017), cyberattacks have dramatically increased.

CHRI's research indicates that during Rouhani's first term (2013-2017), cyberattacks on the social networks accounts of civil and political activists, journalists, academics and influential cultural figures have dramatically increased.

CHRI works directly with individuals under cyberattack to protect their accounts, and as a result, has perspective on the ebb and flow of such attacks. In any given week, CHRI receives on average at least five reports of state-sponsored hacking attacks (most frequently on the mobile messaging application Telegram) from journalists, political activists, women activists and students, with that number rising to an average of at least 20 per week at politically sensitive times such as during the run-up to elections. Given that CHRI comes into contact with only a portion of the state- sponsored hacking attacks undertaken regularly in Iran, these numbers are quite high.

The cyberattacks have not been limited to individuals inside the country, they have also targeted hundreds of civil and political activists outside Iran. Additionally, several public figures within President Rouhani's administration, such as his brother and several deputy ministers of foreign affairs and their families, and others have been the target of cyberattacks.[85]

The methods and patterns used in these cyberattacks and the type of people they have targeted indicates that the hackers have the ability to use the country's telecommunications and communications infrastructure. This means the attackers are state-sponsored.

Two state organizations are responsible for the vast majority of the attacks: the Islamic Revolutionary Guard Corps (IRGC) and, to a lesser extent, the Intelligence Ministry.

In many cases, CHRI has been able to determine the source of the attack due to the methods used. For example, the "high-jacking" of text messages are done by companies owned by the IRGC. CHRI has also interviewed numerous victims of cyberattacks, including those who were arrested on the basis of their online content. These individuals have relayed to CHRI the arresting authorities and the questions asked during the interrogations, information that consistently points to the IRGC.

The nature of the attack varies depending on the motives. The attackers may hack into the account and not disrupt anything, in order to conduct covert surveillance. They may take control of the account and use it to attack someone else's account, or less frequently, to spread false information. When the goal is to stop a website from publishing the news or some piece of information, they will simply bring the website down.

Such surveillance can have catastrophic consequences for the victims. Many journalists and activists in Iran have been prosecuted and sentenced to prison terms for their online communications and activities.

The attacks are usually not technically sophisticated and in some cases, including those that involve Android malware attacks, use tools that can be purchased for approximately $50 USD. Yet they can be effective for hacking individuals who, like most people, are not sufficiently familiar with basic security requirements.

Tactics and Methods

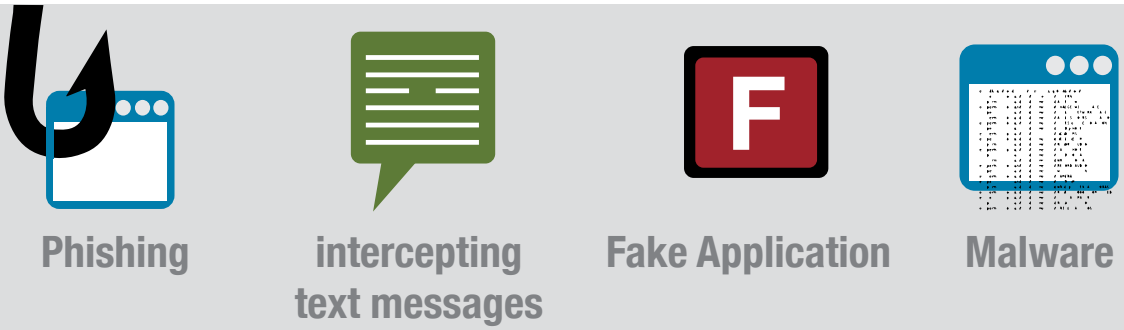
DDoS Attacks

Distributed denial of service attacks (or DDoS) aim to make a website unavailable, and are typically used when the attacker is trying to prevent dissemination of information released on a website.

While DDoS attacks are not one of the tactics most frequently used, they are prominent during politically sensitive times, such as during elections. Over the past four years, the majority of DDoS attacks have targeted the websites of government critics and dissidents inside and outside the country.

The February 2016 parliamentary elections in Iran were the first during Rouhani's presidency in which there was no state-engineered disruption in the country's internet service, but the websites of supporters of reformist and centrist government candidates faced multiple DDoS attacks. During these elections, two websites, the reformist Gaam-e Dovvom and the website of centrist former president Akbar Hashemi Rafsanjani, received the worst of the DDoS attacks, which led to their breakdown.[86]

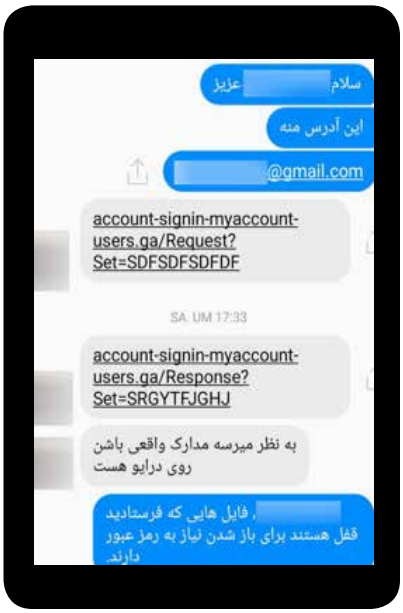
During the presidential election of May 2017, after former president Mahmoud Ahmadinejad (who has fallen deeply out of favor with the supreme leader and other authorities in Iran) was disqualified to run as a candidate by hardline vetting bodies, Ahmadinejad's website was brought down by a DDoS attack, demonstrating that the political proclivities of the victim is not as important as the state of their relationship with the authorities.



TACTICS AND METHODS USED BY STATE-SPONSORED ORGANIZATIONS AND HACKERS

Phishing

Phishing is a type of attack that tricks the users into providing passwords to the victim's account.[87] In this type of attack, the attacker uses information they have about the user, such as their contact list or interests, gains the victim's trust, and then leads the victim to a bait.



An example of penetrating the Telegram account of a reporter by stealing the authentication codes sent via text.

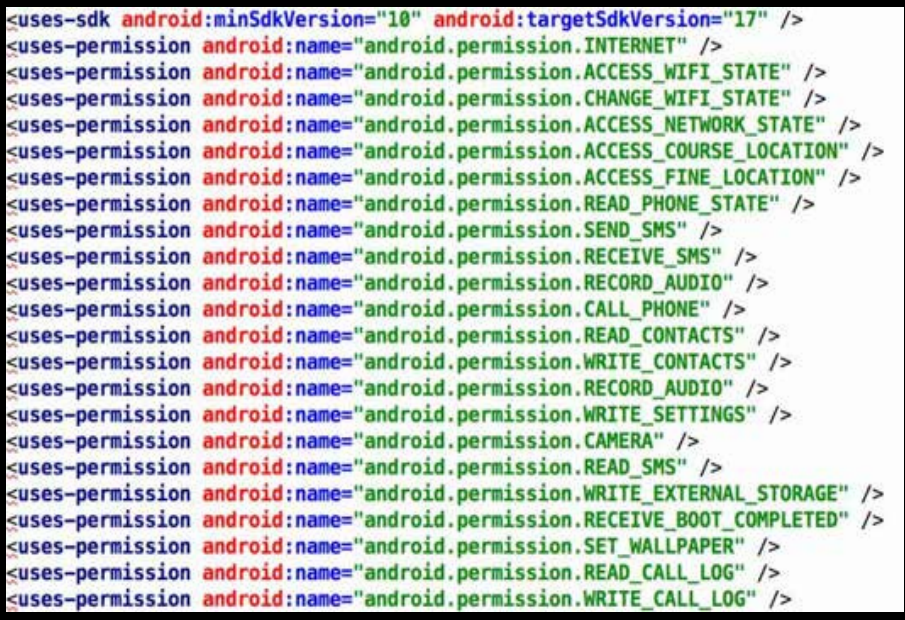
Phishing is one of the oldest techniques used by Iranian intelligence and security forces to access user accounts. Usually this deception is carried out by sending an email, or through a chat on Facebook, or now, increasingly, via the mobile messaging application Telegram, which is heavily used by Iranians. Typically, journalists and activists are targeted, so that the authorities can monitor their communications and contacts, or block the account if they do not have access to the person for questioning (for example if the target resides outside the country and they wish to disrupt communication between that person and individuals inside the country).

In the case of phishing emails, while many email service providers such as Google and Yahoo identify and block these emails, when phishing links are blocked, hackers continuously change their links to attack their targets.

State-sponsored phishing attacks are not limited to users inside the country. For example, in September 2016, the Gmail accounts of Iranian journalists at Radio Farda and Deutsche Welle were successfully attacked.[88]

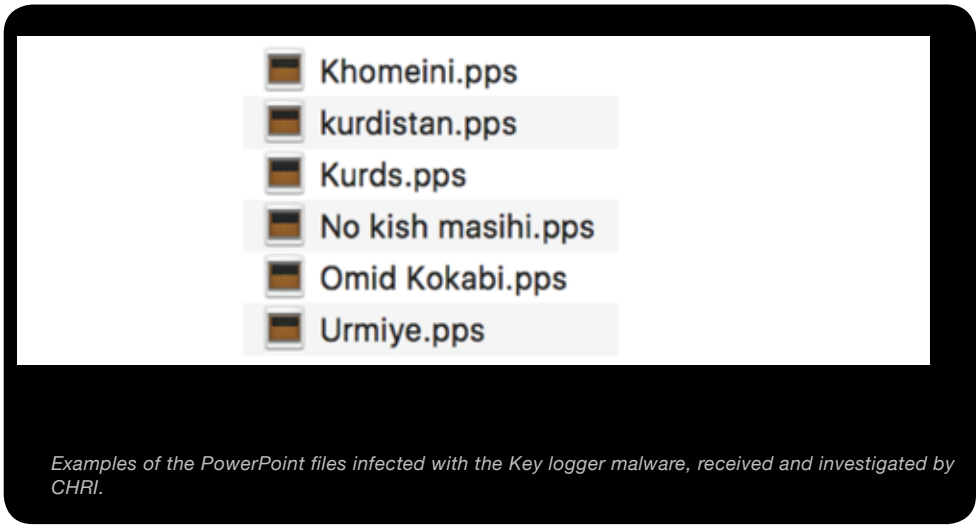
Malware

Malware is a computer program that runs spyware with the aim of collecting information or eavesdropping on the victim after the spyware is installed on a computer or mobile phone. Malware usually allows the attacker to commandeer the victim's computer without his or her knowledge. Malware attacks are heavily used in Iran to monitor, take control of, or block accounts.



This image shows an Android malware analyzed by CHRI. This malware was used to attack a political activist in France.

During the February 2016 parliamentary elections, Hassan Khomeini, the (reformist) grandson of Ruhollah Khomeini, the founder of the Islamic Republic of Iran, was disqualified by hardline vetting bodies from participating in the election. Immediately afterwards, an email containing a PowerPoint file was sent to journalists inside Iran, stating in the body of the email, "Urgent statement by Hassan Khomeini in reaction to his disqualification."[89] Considering the sensitivity and urgency of the subject to Iranian journalists, the hackers knew the file would be quickly and widely opened. As soon as the journalist opened the file, a program named Key logger was installed on the victim's computer, which saved every key pressed on the keyboard and transmitted it to the hacker.



Examples of the PowerPoint files infected with the Key logger malware, received and investigated by CHRI.

According to the Iran Threat's website, which analyzes attacks by Iranian state hackers, there was only one malware attack in Iran prior to the Rouhani administration.[90] Yet from April 2014 to May 2016, CHRI recorded dozens of examples of attacks using this method.

Such malware is generally designed for the Windows operating system, although one example of such malware was also discovered for the Mac operating system.[91] According to a report by the Iran Threats website, this malware, MacDownloader, was previously used to target other countries' infrastructure but has more recently been used to target Mac computers belonging to Iranian human rights activists.[92] MacDownloader steals the user's computer password and creates a fake page where the user types in his or her password in order to enter the computer.[93] It also introduces itself via two fake files for installing the Flash Player[94] software and the Bitdefender[95] Adware Removal Tool. After the user installs the malware, it hides itself in the computer and then makes copies of the database in Keychain Access.

Keychain Access is an application on the Mac OS that allows users to store data such as passwords for emails, websites, Wi-Fi connections, and hardware and software resources that are shared on the network, as well as encrypted disk images of computer memory.[96] In this way, by making a copy of the database program, the hackers gain access to a large part of their victim's information.

Malware is usually not detected by anti-virus programs because the process of finding, reporting and investigating malware by anti-virus companies, and then presenting updated versions of the anti-virus, is a time-consuming process. That, combined with the typical user's lack of basic security knowledge, means that even before these stages are passed, the hackers have already accessed their victims' accounts.

Even in instances where the malware is identifiable by anti-virus software, most users in Iran are using older versions of the anti-virus software and the software will no longer protect them against hacking. Remaining sanctions on Iran and Iranians' difficulty conducting international financial transactions have further hindered their ability to download or buy updated software.

In addition to malware used by state-affiliated hackers to hack Windows and Mac operating systems, over the past two years there has been a substantial increase in malware designed to attack smartphones with the Android operating system, due to the rapidly increasing number of mobile phone users in Iran. After 3G and 4G services were made available to the Iranian public, smartphones and tablets became the main tools for web surfing in Iran. According to a report published on Donya-ye Eghtesad Newspaper on November 29, 2015, there are some 40 million smartphones in Iran.[97] Such a broad market has attracted hackers.

Over the past two years there has been a substantial increase in malware designed to attack smartphones.

For attacking smartphones that use the Android system, hackers now often use tools widely available on the market (that were not intended for malware but can be easily subverted for that use), instead of writing new code to create the malware.[98] According to CHRI research, hackers predominantly use tools such as Metasploit[99] or DroidJack[100] in this regard.

Since the Android operating system, unlike the iOS operating system, allows its users to install Android apps from sources other than certified sources such as GooglePlay, the hackers use different tactics to deceive their victims into installing a fake app that the hackers send.[101]

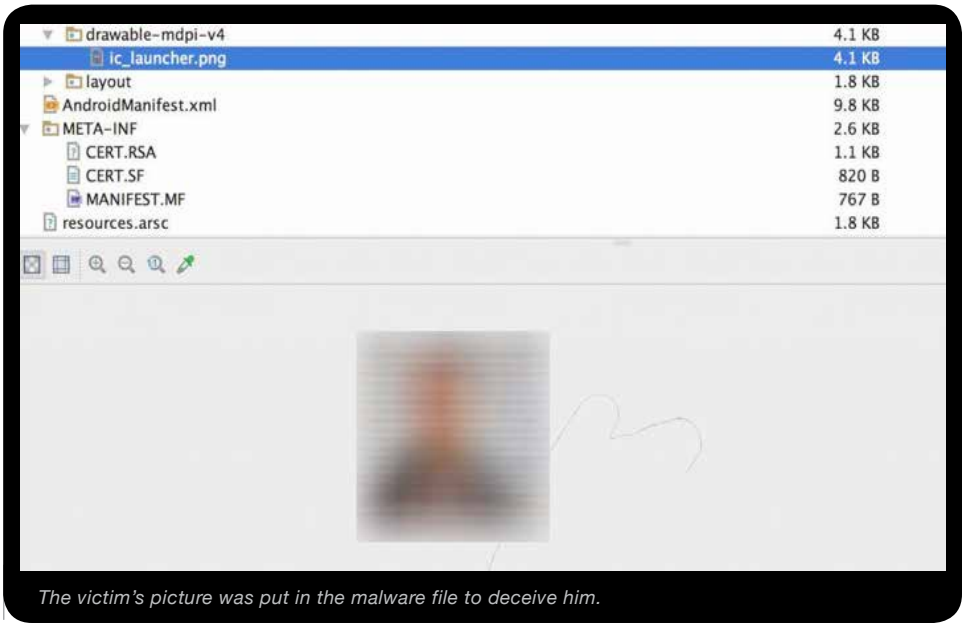
In one example recorded by CHRI, the hacker told the victim that if he used the file sent to him, he would be able to create a safe audio visual connection.[102]

```
<?xml version="1.0" encoding="utf-8"?>
<manifest
    xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="1"
    android:versionName="1.0"
    package="net.droidjack.server"
    platformBuildVersionCode="17"
    platformBuildVersionName="4.2.2-1425461">

    <uses-sdk
        android:minSdkVersion="8"
        android:targetSdkVersion="17" />
```

This image shows the configuration files of the malware CHRI has analyzed. The malware targeted a prominent political activist in Paris. The malware was created using DroidJack.

In another instance, an unknown person contacted a prominent political activist living in France through Facebook and introduced himself as one of his "old students."[103] The hacker said the activist "had done a lot for him," and as a token of his appreciation, he had built him some stickers with his picture for the Telegram application. He sent him a file with the APK[104] extension that contained the picture. Fitting the victim's photo into the file sealed the deception.



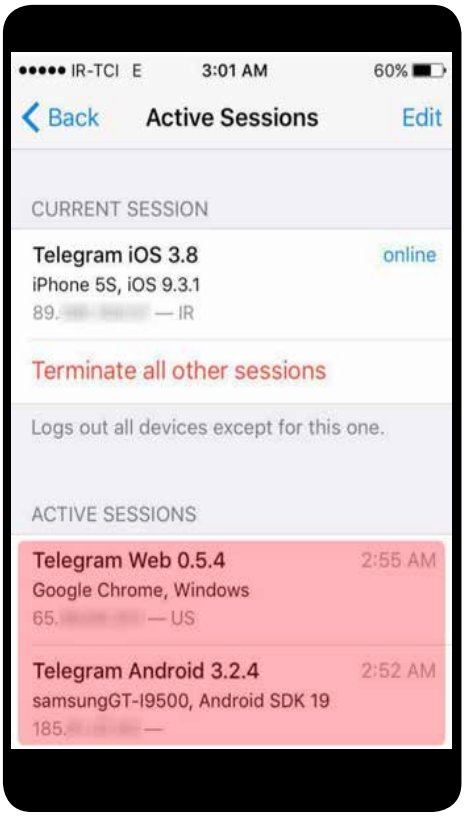
The victim's picture was put in the malware file to deceive him.

In both cases, once the malware was installed, the victim's phone became an online espionage device; every action the victim took was transmitted to the hacker. The hacker was also able to work with the victim's phone. For example, he was able to send text messages, work with any of his applications such as Skype, and even open websites on his browser. The hacker was also able to read his emails and send email messages on his behalf.

All of the attacks using this method that were reported to CHRI targeted individuals such as journalists, civil activists, or political dissidents—in other words, perceived opponents of the state.

Message Tapping

One of the biggest concerns of civil activists and the general Iranian user community over the past two years has become the tapping of text messages by state intelligence and security organizations. The concern is well-founded: many online services such as Telegram, Facebook, and Gmail send access codes as an SMS to authenticate their users and if hackers gain access to these codes, they can easily access the accounts.



An example of unauthorized access to the Telegram account of a journalist in Iran, discovered and analyzed by CHRI.

In this method, hackers who have the phone numbers of their victims go to the login page of the Telegram app, choose "Send code via SMS," tap the user's text messages, intercept the five-digit number the company sends to the user's mobile phone via SMS, and enter the user's account.[105]

Dozens of such attacks on the Gmail, Telegram, Facebook and Instagram accounts of journalists and political activists in Iran have been reported to CHRI by the victims. CHRI's research indicates that the targets of state hacking are chosen due to their political activities, as there is no evidence of any non-political citizens among the victims of this hacking method.

This form of cyberattack is only possible with the cooperation of companies who provide phone services and Iran's Telecommunications Company. It is not possible for anyone except those who have access to these companies and their infrastructure to carry out these attacks. As such, one can conclude these are state-sponsored cyberattacks.

Fake Applications

Another method used to intercept the communications of Iranian users is through the distribution of pirated versions or localized versions of popular applications that are widely used in Iran.

For example, the messaging application Telegram, which has 40 million registered users there, has turned into one of the main sources of news and discourse among Iranians. Unlike other social networks, Telegram also enjoys high popularity among hardline and even radical groups, such as the Basij voluntary militia, and ultraconservative clerics and politicians. Indeed, even those who have held the most vehement stance against other social networks not only have their own news channels on Telegram, but have opposed its blocking.

An example of Fars News Agency's Telegram channel advertisements for Farsi Telegram.

For example, Hasan Abbasi, a hardline ideologue who is close to intelligence agencies and has more than 21,000 members on his Telegram channel,[106] appeared

on a television program in November 2016,[107] where he opposed the blocking of Telegram: "I am a member of Telegram. The legal issues, whether from a morality or a security stand point, remain. In our evaluation and overall assessment, the positive aspect has far outweighed the destructive security aspect…. The medium will come to our help and the [correct] ways of usage will be taught by the people."

Cognizant of the popularity of such applications, state authorities have launched alternative (domestic) mobile social networks. The semi-official Fars News Agency, for example, repeatedly introduced and promoted the capabilities of an alternative application named Farsi Telegram for a month in September 2016 on its Telegram channel. It is worth noting that Fars News Agency's Telegram channel has, as of this writing, never advertised any other products or services and Fars News Agency never accepts advertisements for its Telegram channel or affiliate channels.

CHRI research indicates that Farsi Telegram is in fact a doctored version of the Telegram app in which other capabilities such as phone calls, with the help of open source programs, have been added and made available to the public. (When Farsi Telegram was introduced in 2016, the original Telegram had no voice call capability at that time.) Yet unlike the original Telegram, Farsi Telegram has no encryption and if users use this application, not only would the content of their communications be accessible to intelligence agents, their phone conversations could also be tapped. Telegram CEO Pavel Durov addressed the issue of the compromised security of these fake applications in a tweet on July 29, 2017, in which he responded to another Farsi version of Telegram, Mobogram, stating, "Mobogram is an outdated and potentially insecure fork of Telegram from Iran. I don't advise to use it."[108]

As servers for social media networks or popular foreign instant messaging applications are located outside Iran and Iranian security, intelligence, and judicial organizations have no control over them, over the past two years, Iranian officials have frequently spoken about the necessity of creating and encouraging people to use localized messaging services as an alternative to applications such as Telegram.

For example, on May 28, 2016, referring to a speech delivered by Iran's Supreme Leader Ali Khamenei, Seyed Abolhassan Firouzabadi, Secretariat of the Supreme National Security Council, said, "With the approval of this Council, localized online instant messaging networks which are competitive with foreign messaging apps will be launched within a year."[109]

As of yet such applications have been developed—but have attracted little user interest in Iran. Similarly, the authorities' efforts to pressure foreign companies into placing their servers inside Iran have been roundly refused. The complete loss of user security either option would present has not been lost on the Iranian public, and international companies do not wish to lose their customer base.

Implications

Cyberattacks take place routinely in Iran and are on the rise. Most of the state-sponsored hacking reports CHRI has been receiving have increasingly involved the interception of text messages. Critically, the hackers are using governmental technology infrastructure, namely, the IRGC-owned and controlled Telecommunications Company. As such, it is both within the capacity and the responsibility of the Iranian state to enforce the cessation of such unlawful attacks. Article 25 of Iran's Constitution states, "The inspection of letters and the failure to deliver them, the recording and disclosure of telephone conversations, the disclosure of telegraphic and telex communications, censorship, or the willful failure to transmit them, eavesdropping, and all forms of covert investigation are forbidden, except as provided by law."[110]

Yet these cyberattacks are taking place within an environment of complete immunity. Even members of the Rouhani administration, and family members of cabinet members, have been targeted by cyberattacks, demonstrating that the hackers act at whim against any perceived "opponent."

While Rouhani has publicly addressed many other politically sensitive issues such as corruption, women's rights and even internet access, the president has yet to publicly address the hacking attacks. His silence is an abrogation of his responsibility as president for enforcing Iran's Constitution and defending citizens' rights to privacy. Despite the routine nature of these attacks there is no process or effective institutional mechanism whereby people can file complaints, seek redress, and hold the hackers accountable. In such an environment, civil society is defenseless against these attacks.

Moreover, Rouhani's recent appointment of Mohammad Javad Azari Jahromi as the new Minister of Communications bodes poorly for any administration efforts to address the hacking. Jahromi built parts of the massive state surveillance infrastructure that was used to facilitate the crackdown on the 2009 peaceful protests when he was in the Intelligence Ministry.[111] Under Jahromi, it is difficult to imagine a scenario in which the Communications Ministry will not do the bidding of the intelligence and security agencies.

There is no process or institutional mechanism whereby people can file complaints, seek redress or hold state hackers accountable.

The consequences of these hacking attacks can be catastrophic for the victims. Cyber espionage is being used as a tool for the Iranian judiciary; because the authorities cannot find evidence to legally prosecute the activists, dissidents, journalists and others whom they wish to target, they pursue private information unlawfully obtained through these attacks. They then use this information to prosecute these individuals in sham trials undertaken by a judiciary complicit in the denial of due process and violation of rights.

Filtering

Blocking Under Rouhani

Implications

For as long as the internet has had a presence in Iran, the state has filtered websites and the content on it. However, internet filtering has undergone a transformation during Rouhani's first term (2003-2017).

With the launch of the NIN's national search engines, the Iranian government's ability to filter content has gone from a case-by-case basis to systematic filtering. As discussed in the National Search Engines section of this report, upon detecting any words or phrases that appear on the list of keywords, these national search engines automatically block the content or send the user to fabricated information.

In addition, messaging applications which employ end-to-end encryption, especially those such as the Signal application that do so automatically (with no user input required) have increasingly been blocked, as detailed below.[112] These messaging applications are among the few tools that security and intelligence agencies cannot tap or control through conventional methods, and their inaccessibility to Iranian users has profoundly impacted internet privacy and security in Iran.

In addition to more sophisticated filtering and the blocking of secure messaging applications, authorities have indicated a plan to increase the blocking of social media networks. In a July 18, 2017, meeting with MPs, then Minister of Communications Mahmoud Vaezi announced the launch of four domestically produced social media networks—Salam, Soroush, Wispi and BisPhone—as state-endorsed alternatives to foreign-owned social networks currently used in Iran. "We are waiting for our domestic social media operators to give us assurances that they are ready to launch and then we will get rid of foreign social media networks," he said to the conservative MPs.

The Minister of Communications boasted that 7 million websites were filtered during Rouhani's first term.

The scope of filtering under Rouhani has also been underestimated. In part, as mentioned previously, this is because many filtered sites are still accessible, due to the inability of Iranian filters to "read" (and thus block) encrypted information. This does not, however, mean that the state has tried to roll back any of its filtering activities under Rouhani. Indeed, Rouhani's (previous) Minister of Communications Vaezi's boast that some 7 million websites were filtered during Rouhani's first term indicates the continuation of robust state filtering efforts.[113]

The authorities have sought a further transformation, with the development of so-called "Smart Filtering," designed to filter content selectively as opposed to blocking entire sites. This project was begun during the Ahmadinejad presidency (2005-2013) and has continued under Rouhani.[114] Yet after more than nine years, the project has not had significant success. Because a majority of internet content is transferred between clients and servers in an encrypted manner using SSL security certificates, it is impossible to "read" and thus selectively control its content.

After launching the "smart filtering" project, the filtering of websites and applications is no longer applied at the internet gateway to the country, but rather carried out

by Internet Service Provider (ISP) companies.[115] It would appear this is to prevent a slowdown of network speeds inside Iran, since it is no longer necessary to monitor the entire internet traffic in order to block the targeted websites. This development, however, makes it possible for the ISP to implement its own filtering policies for filtering. This is why for the past two years, many ISP's have not filtered (the officially blocked) Twitter while others continue to filter the application.[116]

The Iranian government has also sought to strengthen its filtering (and online surveillance) capabilities by requiring foreign social media networks to store their Iranian user data in Iran. On August 7, 2017, the country's Supreme Cyberspace Council (SCC) issued a ruling requiring this, and the requirement that foreign companies have a representative based inside the country. Article 2 of the ruling states, "The operational conditions of the messaging services will be prepared and compiled under Telecommunications Ministry guidelines by a working group comprised of representatives from the Ministries of Telecommunications, Culture and Islamic Guidance, and Intelligence, as well as the president's office, the prosecutor general's office, the Islamic Propagation Organization, the cyber police force, and the Islamic Revolutionary Guard Corps." So far, no foreign company has complied with this requirement.

The Iranian government has sought to strengthen its filtering and surveillance capabilities by requiring social media networks to store their Iranian user data in Iran.

Blocking Under Rouhani

The Rouhani administration's record on blocking sites has also not supported his stated support for internet freedom. To be sure, his administration has on several occasions resisted the blocking of social networks. For example, as previously mentioned, in 2014 Rouhani issued an order to ban the blocking of the WhatsApp messaging application, and, in the run-up to the February 2016 parliamentary elections in Iran, he refused requests by police and security forces to block popular messaging services such as Telegram. (During those elections, pro-Rouhani, centrist and reformist political channels were prominent on Telegram.)

Overall however, the blocking of services and applications has quietly accelerated under Rouhani, and this has had significantly negative implications for online security in Iran. During his first term, many secure messaging applications and secure search engines were filtered and made inaccessible to users (see list below). The authorities provided no explanations for the blocking of these services.

Critically, the bulk of the restrictions have been imposed on tools for maintaining digital security and privacy, such as the aforementioned applications that provide encryption by default, enabling users to store and carry out correspondence, searches, and files in a safe environment.

For example, the DuckDuckGo[117] search engine, which is an open source search engine widely regarded as a secure tool for maintaining the privacy of its users, was filtered and blocked during Rouhani's first term.

Some of the other major sites filtered during Rouhani's presidency have included security websites, messaging apps, search engines, and online games. They include:

1. Signal secure messaging application
2. Popular game Pokémon GO
3. Google Play App Store
4. CryptoCat secure chat application
5. Kik messaging application
6. DuckDuckGo secure search engine
7. Periscope video broadcasting tool on Twitter
8. Google Drive
9. Netflix
10. Russian search engine Yandex
11. The Omid List website (which contained a list of reformist candidates for Iran's Parliamentary elections)
12. Dropbox file sharing website
13. Website of author Mohammaed Ghaed
14. Pinterest website for photo sharing
15. Bitly link shortening website
16. Steam comunity marketplace for computer games
17. Origin marketplace for computer games
18. Footballitarin sports website
19. Imo messaging app
20. Wechat messaging app
21. http://www.quora.com question and answer website
22. Euronews' news website http://persian.euronews.com was filtered,[118] which was later changed to http://fa.euronews.com and the present address is not filtered.
23. The movie db film poster website
24. Blogger and Blogspot, Google Company blog services http://onedrive.live.com

As stated previously, the use of SSL security certificates makes it impossible for the filtering system to "read" the content, allowing many of the sites listed above to remain accessible despite being blocked. As a result, many observers have underestimated the extent to which filtering has continued and even accelerated under the Rouhani administration.

For sites focused on areas in which the authorities in Iran are extremely sensitive, such as human rights organizations (for example, CHRI) or social media networks widely used by activists and critics of the government (such as Facebook), the government institutes a more technically sophisticated blocking mechanism that the SSL cannot circumvent, based on the website IP address and TLS inspection. In this manner, such sites remain blocked in Iran, despite their use of an international SSL certificate.

The Working Group to Determine Instances of Criminal Content has also barred Iranian mobile app stores from offering applications to the public that are blocked in Iran. For example, Reza Mohammadi, the Technology Department Head of Cafe Bazaar, the most popular Android app store in Iran, said in a tweet that the IMO app had been removed from the online store's list by order of the committee, referencing the third paragraph of the Law on Cyber Crimes.[119]

Reza Mohammadi, Technology Director of Cafe Bazaar, said in response to a tweet: The IMO application was removed from Cafe Bazaar on orders from the Committee to Determine Instances of Criminal Content.

According to this paragraph, "publishing links or promoting filtered websites or re-publishing criminal content of banned publications and media affiliated with groups and deviant and illegal organizations" is against the law and banned.[120] In accordance with this law, none of the other popular blocked applications such as Twitter, Facebook, YouTube, or secure messaging apps such as Signal, are available for sale in Iranian stores.

Moreover, during important periods such as elections in Iran, filtering and blocking has increased. For example, during the run-up to the February 2016 parliamentary elections, a video made by reformist former Iranian President Mohammad Khatami published on the Aparat website (announcing his support for reformist candidates) was removed on orders from the Committee to Determine Instances of Criminal Content, which cited Article 23 of the Law on Cyber Crimes.

Article 23 does not refer to content and only states, "Providers of web hosting services shall upon receipt of instructions from the working group that determines the instances mentioned in the above article, or the judicial authority reviewing the case for existence of criminal content in its computer systems, bar access to it" and in case of disobedience, they will face cash fines and a ban on activities.[121]

Also during the February 2016 campaigning, content filtering on Instagram was more aggressive, via identifying user accounts, keywords and hashtags. Numerous user accounts which contained content concerning human rights or political activities were blocked. For example, access to hashtags that contained the names of Seyed Hassan Khomeini (the reformist grandson of the founder of the Islamic Republic of Iran Ruhollah Khomeini), former reformist President Mohammad Khatami, and centrist former President Akbar Hashemi Rafsanjani were blocked, as were the hashtags referencing political prisoners such as #freejason, #jasonrezaian and #freearashzd.

Under Rouhani, internet filtering in Iran has increased in scope and sophistication.

During this period, the Omid (Hope) website, which provided a list of reformist candidates, was blocked as well. During the February 2016 parliamentary elections, Instagram hashtags were filtered, but because of Instagram's encryption, the filtering had no impact and images were still displayed for the users.

In April 2017, weeks before Iran's May 2017 presidential election, Telegram's Voice Call was blocked, based on a judicial order that cited the "national security" implications of their encrypted connection. Also in April 2017, Instagram Live, which had been used heavily to broadcast reformist political events, was blocked, without explanation or official comment.

Last and most recently, in December 2017, Instagram and the Telegram messaging app were completely blocked after unrest broke out throughout the country. In this instance, the government employed its more sophisticated blocking mechanism that an SSL cannot circumvent, based on the website IP address and TLS inspection. In addition, access to VPNs and other circumvention tools were blocked.

Image of Mohammad Khatami's deleted video from Aparat website, considered a replacement for YouTube in Iran.

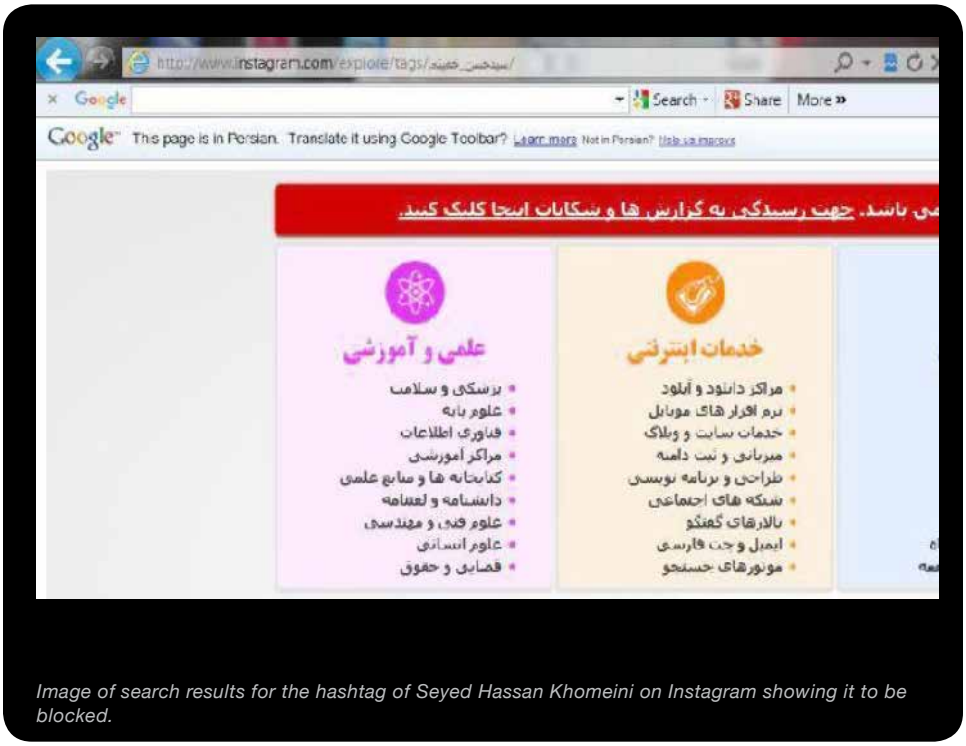


Image of search results for the hashtag of Seyed Hassan Khomeini on Instagram showing it to be blocked.

Implications

Under Rouhani, internet filtering has not only continued, it has been strengthened. National search engines now allow systematized filtering and re-direction to state-approved (and often falsified) content. The blocking of major social media platforms, especially during sensitive times such as elections or during unrest, has continued, as recent events have demonstrated. Blocking services and applications that provide encryption by default has also intensified. These tools and services provide a lifeline for Iranians trying to maintain internet access and privacy. The inability to access these tools from Iranian stores, or buy them internationally due to constraints on international financial transactions with Iranians, has meant Iranians are deprived of tools vital to their internet access and security. Indeed, under Rouhani, Iran's most complex and costly national project for internet censorship and control—the NIN—has significantly advanced, and with it, Iranians' ability to access the global internet is now subject to state discretion. Overall, internet use in Iran has expanded during Rouhani's tenure, but internet freedom certainly has not.

Conclusion

Iranians' most basic rights are being violated. Internet access and privacy have become integral to the fundamental human rights of freedom of speech, expression and association, the right to access information, and the right to privacy. Yet with the development of the NIN, which has advanced considerably under the Rouhani administration, Iranians are being subjected to an increasingly sophisticated system of online control, censorship and surveillance. Their ability to freely access information and a secure means of communications is becoming more difficult. Indeed, their very ability to access the global internet, and with it, information that is not state-approved, is now dependent upon state will. State-sponsored hacking in Iran is also accelerating and being routinely used to unlawfully obtain "evidence" to prosecute individuals—without public protest or comment by President Rouhani.

The right to privacy is specifically referenced in Iranian law yet it is violated with impunity in Iran by intelligence and security officials who work hand in hand with the judiciary to exert control over the citizenry and punish whomever they believe challenges that control. In this they have the robust support of Iran's supreme leader, Ali Khamenei, who views the internet as a Western-inspired plot to weaken the Islamic Republic. While the Rouhani administration pays lip service to the vital role of digital communication in modern life, and has in some respects supported this role by upgrading the technical infrastructure in Iran, it has proceeded steadily with state initiatives that are significantly expanding online control and surveillance and has remained silent in the face of intensified state hacking.

In such an environment, peaceful dissent, another basic right under Iranian and international law, is undermined and carries grave risk. The numerous Iranians sitting in prisons throughout the country after trials that lacked any semblance of due process and based on unlawfully obtained online content attests to this. It is incumbent upon those in Iran who support the rule of law, as well as those in the international community who accept the responsibility to defend citizens' rights wherever they are, to speak out forcefully against such policies and inform Iranian state officials that they are unacceptable. It is also imperative for governments worldwide, the United Nations, and the technology sector to fully support the Iranian people's efforts to access a free, open and safe internet, and the tools and services that support that access. Internet freedom and freedom are now one and the same.

Endnotes

1 "The limitation of 128 kb speed for home use was lifted," Khabar Online, May 5, 2013 http://goo.gl/ZNrqRb

2 "Internet in Chains: The Front Line of State Repression in Iran," Center for Human Rights in Iran, November 17, 2014 https://www.iranhumanrights.org/2014/11/internet-in-chains

3 Statements made during the meeting of president and cabinet members, Seyed Ali Khamenei's website, November 17, 2016 https://goo.gl/fpPIuO

4 "Khamenei Consolidates Power over Internet Policy in Hard Line Council He Controls,"September 14, 2015 https://www.iranhumanrights.org/2015/09/khamenei-internet-policy-iran/

5 "Meet High Council of Informatics," Hamshahri Newspaper, August 6, 2010 https://goo.gl/WnHMfq

6 Ibid

7 "The Dissolution of the High Council of Informatics and AFTA and their Merger in the Supreme Council of Cyber Space," Khabar Online, April 12, 2016 https://goo.gl/0mKN6P

8 "Khamenei Consolidates Power over Internet Policy in Hard Line Council He Controls," September 14, 2015 https://www.iranhumanrights.org/2015/09/khamenei-internet-policy-iran/ https://goo.gl/7jxrxP

9 "Ten Things You Should Know About Iran's Multi-Billion Dollar National Internet Project," Center for Human Rights in Iran, October 13, 2016 https://www.iranhumanrights.org/2016/10/ten-things-you-should-know-about-irans-national-internet-project/

10 "National Information Network documents," Ministry of Communications website https://goo.gl/83sfNs

11 CHRI cannot identify these sources for security reasons, but they participated directly in these meetings and communicated this information to CHRI in detailed interviews afterwards.

12 "President orders removal of filtering on WhatsApp," Mehr News Agency, May 6, 2014 https://goo.gl/4tbgiQ

13 "The limitation of 128 kb speed for home use was lifted," Khabar Online, May 15, 2013 http://goo.gl/ZNrqRb

14 "Rouhani: I am dissatisfied with the bandwidth conditions in the country," ILNA News Agency, May 17, 2014 https://goo.gl/p5mKwM

15 “Where is the law?!” Kayhan Newspaper, May 18, 2014 https://goo.gl/eAZT4z

16 “Communications Minister: ‘Certain agencies pressured us for filtering of social networks and Internet disruption, but we resisted,’” Khabar Online, February 26, 2015 https://goo.gl/GMFDdM

17 “Where is the law?!” Kayhan Newspaper, May 18, 2014 https://goo.gl/eAZT4z

18 “Iranian Judiciary Blocks Popular Telegram App’s New Voice Call Service,” Center for Human Rights in Iran, APRIL 20 2017, https://goo.gl/7yutys

19 “The Positive and Negative Functions of internet in Viewpoint of Ayatollah Khamenei,” Mashregh News Website, November 5 2013, https://www.mashreghnews.ir/news/261243

20 “Deputy Prosecutor General: Smart filtering is ineffective”, Fars News Agency, September 6 2015, http://www.farsnews.com/newstext.php?nn=13940615001311

21 Signal website https://whispersystems.org

22 Crypto Cat website https://crypto.cat

23 DuckDuckGo website https://duckduckgo.com

24 “Rouhani Government “Closed Seven Million” Websites in First Term”, Center for Human Rights in Iran, June 8 2017, https://goo.gl/n8euB9

25 “Hackers Exploit Android Phone Security Flaw to Target Activists,” Center for Human Rights in Iran, August 31, 2016, https://www.iranhumanrights.org/2016/08/increase-android-malware-attack/

26 “Revolutionary Guard’ Cyber Attacks Now Directed at Rouhani Cabinet Members,” Center for Human Rights in Iran, April 26, 2016 https://www.iranhumanrights.org/2016/04/cyber-attacks-iranian-officials/

27 “Rouhani Unveils Toothless Charter on Citizen’s Rights Without Path to Implementation,” Center for Human Rights in Iran, December 22, 2016 https://www.iranhumanrights.org/2016/12/rouhani-citizens-bill-of-rights/

28 “Ten Things You Should Know About Iran’s Multi-Billion Dollar National Internet Project,” Center for Human Rights in Iran October 13, 2016 https://www.iranhumanrights.org/2016/10/ten-things-you-should-know-about-irans-national-internet-project/

29 “Deputy Minister of CIT: Third phase of National Information Network will be implemented by the end of [Rouhani] presidency,” Tasnim News Agency, February 7, 2017 https://goo.gl/MgMZRf

30 “Final phase of National Information Network delayed,” IT Analysis website, April 3, 2017 https://goo.gl/O3tqiz

31 National Information Network website https://goo.gl/s7ZntS

32 E-Government website http://egovernment.ir

33 This service would allow the users to load their suspicious files onto it, as they would on the similar non-Iranian versions of Virus Total, in order to test them for viruses and malware.

34 "Asiatech Managing Director describes the method for calculating Internet and Intranet access rates," ILNA News Agency, March 11, 2017 https://goo.gl/56X1Zq

35 http://www.asiatech.ir

36 https://www.rightel.ir

37 https://irancell.ir

38 "MOU signed for reducing rates for internal Internet traffic," Asiatech Company website, June 2016 https://goo.gl/gJxMLr

39 https://www.tic.ir

40 http://www.aparat.com

41 http://www.filimo.com

42 http://www.telewebion.com

43 http://razavitv.aqr.ir/index

44 Global net neutrality Coalition, https://www.thisisnetneutrality.org

45 UN expert demands urgent boost for online rights amid rampant State censorship," Office of the United Nations High Commissioner for Human Rights, June 12 2017, https://goo.gl/MLvzmS

46 "The second phase of the National Information Network was launched," Zoomit website, February 6, 2016 https://goo.gl/gJs3z3

47 Measurement Lab, https://viz.measurementlab.net

48 "22 million Iranians use mobile Internet," Mehr News Agency, September 20, 2016 https://goo.gl/umsiJJ

49 "New Report Reveals State's Growing Efforts to Control Internet Access in Iran," Center for Human Rights in Iran, November 17 2014, https://www.iranhumanrights.org/2014/11/internet-in-chains

50 "Internet exchange points list," Infrastructure Company, https://www.tic.ir/fa/ixp-centers

51 Tehran Internet Exchange Points, http://tehran-ix.ir

52 Qom Internet Exchange Point, http://tehran-ix.ir/fa/qom-ixp

53 Mashhad Internet Exchange Points, http://mashhad-ix.ir

54 Shiraz Internet Exchange Points, http://shiraz-ix.ir

55 Tabriz Internet Exchange Points, http://tabriz-ix.ir

56 "Revolutionary Guard' Cyber Attacks Now Directed at Rouhani Cabinet Members," Center for Human Rights in Iran, April 26 2016, https://www.iranhumanrights.org/2016/04/cyber-attacks-iranian-officials

57 "All users to be authenticated in National Information Network," IT Iran website, August 28 2016, https://goo.gl/aTg8f0

58 "All users to be authenticated in National Information Network," IT Iran website, August 28, 2016 https://goo.gl/aTg8f0

59 Ibid https://goo.gl/3SWK8w

60 "Separating National Information Network and Internet User traffic, "Eghtesad Online Website, September 31, 2016 https://goo.gl/1IoWws

61 Chapar Email website https://chmail.ir

62 "Iranian Judiciary Must Stop Punishing Media for Reporting Officials' Corruption," September 9, 2016, https://goo.gl/5tNA8f

63 In broadcasting, over-the-top content (OTT) is the audio, video, and other media content delivered over the Internet without the involvement of a multiple-system operator (MSO) in the control or distribution of the content.

64 "Iranians Looking Abroad to Escape State-Controlled Internet," March 14, 2016, https://goo.gl/XGB1mh

65 Saina web site, http://saina.ito.gov.ir

66 "Full text of e-commerce law," ITNA News Agency, November 14 2015, https://goo.gl/Wjac67

67 Governmental Center for Root Certificate Authority, http://www.rca.gov.ir

68 "The number of downloaded Saina exceeded to 440,000 downloads," Saina Web Site http://goo.gl/7WYTWR

69 "Chapar" is the name of an email designed and launched by Fanavaran Bartar Andish Farasp.

70 "A new replacement for Iranian email services," IT Analysis website, November 30,

2015. https://goo.gl/sivzqY

71 Since 2013, this software has been used as the new email service for Amirkabir University of Technology, using a French security certificate.

72 Perfect Forward Secrecy

73 “Government site hack confirmed!” May 28, 2016, Asr-e Iran website https://goo.gl/YlRg9G

74 DotNetNuke is a web content management system based on Microsoft .NET. The DNN Platform Edition is open source

75 “Launch of Data Centers by government organizations will be prohibited,” Mehr News Agency, December 7, 2016 https://goo.gl/Rk9idp

76 “CIT Minister: The Chinese’s request to build data centers in Iran,” ISTNA website, February 8, 2016 http://goo.gl/bVfHha

77 “Why don’t Iranians use Iranian search engines?” Khabar Online, March 2, 2015 https://goo.gl/AOhHwL

78 “The unequivocal response of Deputy Minister of ICT to criticism of national search engines,” ISNA, February 24, 2015 http://goo.gl/FXbdYn

79 “Invitation to continue implementation of national search engines,” IT Analysis website, May 9, 2015 http://goo.gl/cblUK1

80 “Will Yandex be the replacement filter for Google?” IT Analysis website, October 26, 2015 http://itanalyze.com/post/29701

81 Yandex website https://www.yandex.com

82 “The Supreme Leader appoints Dr. Ali Asgari to head the IRIB,” Supreme Leader’s website, May 11, 2016 https://goo.gl/i0D68F

83 “National Operating System Document approved/Linux to replace Farsi Windows,” Mehr News Agency, April 28, 2010 https://goo.gl/yvUFbb

84 “Local Operating System to be launched,” Asr-e Iran, September 28, 2015 http://goo.gl/tlywYV

85 Revolutionary Guard’ Cyber Attacks Now Directed at Rouhani Cabinet Members, Center for Human Rights in Iran, April 26, 2016 https://www.iranhumanrights.org/2016/04/cyber-attacks-iranian-officials

86 “Concern expressed over involvement of supervisory bodies for the annulment of some ballot boxes in northern Tehran,” Center for Human Rights in Iran, February 25, 2016 https://goo.gl/FQ9CUs

87 "Android Phone Users in Iran Face New Threat by Hackers," Center for Human Rights in Iran, August 16, 2016 https://www.iranhumanrights.org/2016/08/fake-imo-app

88 "Hackers Exploit Android Phone Security Flaw to Target Activists," Center for Human Rights in Iran, August 31, 2016, https://www.iranhumanrights.org/2016/08/increase-android-malware-attack

89 Revolutionary Guard' Cyber Attacks Now Directed at Rouhani Cabinet Members, Center for Human Rights in Iran, April 26, 2016 https://www.iranhumanrights.org/2016/04/cyber-attacks-iranian-officials

90 Iran Threat website https://iranthreats.github.io/us-16-Guarnieri-Anderson-Iran-And-The-Soft-War-For-Internet-Dominance-paper.pdf

91 "Report: Iranian Hackers Target Activists' Mac Devices With Revamped Malware," Center for Human Rights in Iran, February 12, 2017 https://www.iranhumanrights.org/2017/02/macos-malware-targeting-iranian-hr-activists

92 "IKITTENS: Iranian Actor Resurfaces with Malware for Mac (MacDownloader)," Iran Threats, February 6 2017, https://goo.gl/Q4I8sC

93 MacDownloader

94 Flash Player

95 Bitdefender Adware Removal Tool

96 Encrypted disk images

97 "The rapid growth of smartphone users in Iran," Donya-ye Eghtesad Newspaper, November 29, 2015 https://goo.gl/SGBpXN

98 "Hackers Exploit Android Phone Security Flaw to Target Activists," Center for Human Rights in Iran, August 31, 2016, https://www.iranhumanrights.org/2016/08/increase-android-malware-attack

99 Metaspoilt website https://www.metasploit.com

100 DroidJack website http://droidjack.net

101 Google App Store https://play.google.com/store

102 "Hackers Exploit Android Phone Security Flaw to Target Activists," Center for Human Rights in Iran, August 31, 2016, https://www.iranhumanrights.org/2016/08/increase-android-malware-attack

103 Ibid

104 APK is the extension for Android application package files.

105 "Negligence by Major Tech Companies like Google and Telegram Aiding Iran's

Cyber Army," Center for Human Rights in Iran, June 3, 2016 https://www.iranhumanrights.org/2016/06/state-sponser-hacker-and-google-telegram

106 Hasan Abbasi's Telegram channel https://telegram.me/hasanabbasi_students

107 "Dr. Hasan Abbasi on blocking Telegram," video from Aparat website, November 19, 2015 https://goo.gl/27z3TV

108 "Mobogram is an outdated and potentially insecure fork of Telegram from Iran. I don't advise to use it." Pavel Durov twitte, July 29 2017, https://twitter.com/durov/status/891213634248085505

109 "Localized instant messaging networks will be launched," IRIB News Agency, May 28, 2016 https://goo.gl/6n3aol

110 The Constitution of the Islamic Republic of Iran, www.alaviandassociates.com/documents/constitution.pdf

111 "Rouhani Cabinet Pick Linked to Mass Surveillance of 2009 Protestors," Center for Human Rights in Iran, August 16, 2017 https://www.iranhumanrights.org/2017/08/rouhani-cabinet-pick-linked-to-mass-surveillance-of-2009-protesters/

112 End to End Encryption

113 Rouhani Government "Closed Seven Million" Websites in First Term, Center for Human Rights in Iran, June 8, 2017 https://www.iranhumanrights.org/2017/06/rouhani-government-closed-seven-million-websites

114 The first phase was launched on May 16, 2015, and the second phase was launched on November 9, 2015.

115 "Smart Filtering reaches third phase," Zoomit website, March 7, 2016 https://goo.gl/tQ4HJa

116 "Briefing: Tracking Twitter's Growing Popularity in Iran," Center for Human Rights in Iran, February 21, 2017 https://www.iranhumanrights.org/2017/02/briefing-twitter-third-wave-in-iran

117 DuckDuckGo search engine http://www.duckduckgo.com

118 "Euro news Farsi website filtered!" Parsineh website, April 11, 2016 https://goo.gl/URWQsN

119 Tweet from Reza Mohammadi, Head of Cafe Bazaar's Technology Department https://goo.gl/sNaM49

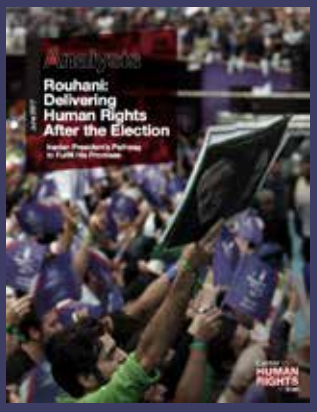
120 Law on Cyber Crimes http://internet.ir/law.html

121 Ibid

Guards at the Gate: *The Expanding State Control Over the Internet in Iran* by the Center for Human Rights in Iran (CHRI) provides an in-depth analysis of the Iranian government's growing capabilities to censor, monitor and control use of the internet in Iran. The report offers a comprehensive review of Iran's state-controlled National Internet Network (NIN), which gives the government critical new abilities to filter the internet, identify users, hack into private accounts, and cut Iranians off from the global internet while maintaining access to domestic online sites and services—a capacity demonstrated briefly for the first time during the December 2017-January 2018 unrest in Iran. In addition to analysis of the technological advancements and policy initiatives the government has undertaken over the last five years, the report also offers discussion of the tools and methods of the intensifying state-sponsored cyberattacks in Iran. Building on years of extensive research and reporting by CHRI on internet issues in Iran, Guards at the Gate provides a full understanding of the implications these new capabilities have for Iranians' internet freedom and security.

Recent reports

by the Center for Human Rights in Iran



Rouhani: Delivering Human Rights After the Election
MAY 25, 2017

Hassan Rouhani was re-elected as president of Iran in May 2017 largely on the basis of his support for human rights and Iranians' perceptions that he would do more to improve civil and political rights in the country than his rivals. He should now deliver on his pledges.

Briefing: Iran's Fashion Industry is the Latest Victim of Khamenei's War on Western Culture
DECEMBER 8, 2016

Iran's brain drain has spread to the fashion sector as designers, photographers, models and other industry professionals emigrate to escape raids, the shuttering of their businesses, arrests and prosecutions under vague laws that restrict freedom of expression.

Inside the Women's Ward: Mistreatment of Women Political Prisoners at Iran's Evin Prison
JUNE 20, 2016

Political prisoners held in the Women's Ward at Iran's Evin Prison are routinely denied medical care and hospitalization, face restricted or denied visitation rights even with their young children, are deprived of regular telephone contact with their families, and are not provided adequate nutrition, as documented in this report.