المـركز العـربي للأبحـاث ودراسة السيـاسات
Arab Center for Research & Policy Studies

Case Analysis | 8 May 2022

Information Controls in Iranian Cyberspace: A Soft War Strategy

Melinda Cohoon

The Iranian Studies Unit

Information Controls in Iranian Cyberspace: A Soft War Strategy

Series: Case Analysis

8 May 2022

Melinda Cohoon

The Iranian Studies Unit

Melinda Cohoon

A PhD Candidate in the Near and Middle Eastern Studies program at the University of Washington. Her work focuses on information controls, gamers, and the video game industry in Iran and in the diaspora. Funded by the Roshan Institute Fellowship for Excellence in Persian Studies and the Social Science Research Council's Social Data Dissertation Fellowship, her dissertation titled "Affective Entanglements: Iranian Gamers on Social Media and Online Games" uncovers how the everyday experience of sanctions and censorship produce precarious emotions, sentiment, and belonging for Iranian gamers online. She also has extensively worked on digital humanities projects, leading to the *IDEAH* journal publication "Digital Iran: Soft Power and Affect in Video Games" (2020).

The Arab Center for Research and Policy Studies is an independent research institute and think tank for the study of history and social sciences, with particular emphasis on the applied social sciences.

The Center's paramount concern is the advancement of Arab societies and states, their cooperation with one another and issues concerning the Arab nation in general. To that end, it seeks to examine and diagnose the situation in the Arab world - states and communities- to analyze social, economic and cultural policies and to provide political analysis, from an Arab perspective.

The Center publishes in both Arabic and English in order to make its work accessible to both Arab and non-Arab researchers.

The Arab Center for Research and Policy Studies
Al-Tarfa Street, Wadi Al Banat
Al-Dayaen, Qatar
PO Box 10277, Doha
+974 4035 4111
www.dohainstitute.org

Table of Contents

Cyberspace is a global symbolic space where things happen on the internet. It is also the virtual reality where people translate the meaning of images, words, and video, communicate with one another via instant messaging or email, play virtual games, create websites, and even build virtual worlds based on fictional or real-life places. Although the Iranian internet consists of "many places" that are not necessarily "'Iranian' in any straightforward way," Iranian Cyberspace has particular nuances related to the lived experiences of Iranian citizens and the political choices the government makes.[1] As such, Iranian Cyberspace can be described as many online places existing in an all-encompassing global cyberspace, where embodied Iranian citizens extend their online selves in socio-political and cultural ways across digital platforms and virtual worlds. Several Iranian government entities also extend themselves across cyberspace to achieve cyber suppression of Iranian citizens through oppressive measures and legal conditions, including but not limited to aggressive online attacks, imprisonment, violence, filtered internet (filternet), deliberately slowing down internet speeds (throttling), and full internet blackouts. Iranian Cyberspace is therefore an existential space and a real context that specifically relates to the socio-cultural experience of citizens and government information controls. This information control strategy is predicated not only on the expansion of soft power in Iran and across the globe, but also on soft war, or *jang-e narm*.

While the Islamic Republic of Iran undoubtedly uses cyberspace for censorship and surveillance of its citizens, including cyber warfare to damage information systems outside of Iran, its cyber suppression strategy of soft war seeks to curtail the flow of information through the internet to prevent "the spread of foreign ideas, culture, and influences through information communication technology" into Iran.[2] Soft war is a strategic method of information control that explicitly prohibits outsiders, such as Western states, and specifically the United States, from accessing information and simultaneously preventing the spread of Western information among Iranian citizens. In addition to spreading disinformation, the government's information control strategy of soft power seeks to curate its state narrative through its ideological campaign inextricably linked to its Persian imperial legacy, myths, and history, or in other words, the control of culture.[3] Iran's conservative agenda towards controlling information has come to the fore with its most recent attempt to cut Iran off from cyberspace with the "Bill for Protection of Cyberspace Users." Because of US sanctions, Iranians are prohibited from accessing major technology tools and online spaces such as Amazon, Google, Apple, and online multiplayer games like World of Warcraft, effectively severing Iranians from cyberspace. Doubly so, Iranians already experience the government's soft war and soft power initiative to further cut them off from global cyberspace. US sanctions make it easier for surveillance and censorship in Iran since it removes citizen access to various online platforms, software, and tools. Iranian citizen internet freedom continues to be threatened with mounting support for "Bill for Protection of Cyberspace Users," which would establish a truly domestic internet walled off from global cyberspace.

[1] Niki Akhavan, *Electronic Iran: The Cultural Politics of an Online Evolution* (New Brunswick: Rutgers University Press, 2013), p. 2.

[2] E.L. Blout, "Soft War: Myth Nationalism, and Media in Iran," *The Communication Review*, vol. 20, no. 3 (2017): p. 212.

[3] Seth G. Jones and Danika Newlee, "The United States' Soft War with Iran," *Center for Strategic and International Studies*, June 11, 2019, https://bit.ly/37DjUhb.

Iran’s Bureaucratic Internet Infrastructure

Iran’s history of controlling information through censorship from around the globe and in local news media has been evident since its founding in 1979. However, with the advent of the internet in the 1990s, in combination with the tensions between several bureaucratic agencies in Iran, the state focused on quality and access to network services.[4] It was during the growth of internet cafes in the early 2000s that the popularity of blogging became a powerful means to communicate political opposition to the state, leading to the incarceration of bloggers like Sina Motallebi in 2003 and Hossein Derakhshan in 2008, as well as the intensification of internet information controls. Following proposals in 2005 to reduce dissent from bloggers, Supreme Leader Ayatollah Ali Khamenei ordered the creation of a bureaucratic center of national intranet called the National Information Network (NIN) to develop an Iranian national internet network with infrastructure that delivers services to the public and private sector in 2006. Essentially, through switches, routers, and data centers, NIN prevents outsiders from having access to the Iranian Cyberspace while also encouraging the Iranian public to consume domestic websites and social media. As a multi-billion-dollar internet project, the Iranian government’s NIN program maintains the functionality of the internet through search engines, email, and news outlets, or rather domestic filternet, while also throttling international internet traffic - especially during protests. International embargoes, from the United States maximum pressure campaign to sanctions, have also forced NIN to become more sophisticated in its strategies over the years, especially to prevent foreign interference while simultaneously increasing internet speeds.[5] This has manifested in an Iranian national security policy of soft war and hard power responses (e.g. violence and prison sentences) towards citizens by forcing them to use NIN.[6] And while NIN curates and monitors the internet, the Iranian government’s infrastructure for information controls consists of severely conflicting goals as it seeks to increase internet speed by expanding bandwidth through its Telecommunication Company of Iran (TCI).[7]

To maintain geopolitical control and increase territorialization of Iranian Cyberspace through soft war, NIN is but one government entity in Iran that assists in the strategic competition and regional influence over internet surveillance and censorship. Active measures are also taken by several government entities including the Iranian Cyber Police, Supreme Council of Cyberspace, Cyber Defense Command, National Passive Defense Organization, National Cyberspace Center, Islamic Revolutionary Guard Corps (IRGC, Sepah), IRGC Electronic Warfare and Cyber Defense Organization, and the Basij Cyber

[4] Babak Rahimi, “Cyberdissent: The Internet in Revolutionary Iran,” *Middle East Review of International Affairs*, vol. 7, no. 3 (2003): p. 102.

[5] Loqman Salamatian, Frédérick Douzet, Kavé Salamatian, and Kévin Limonier, “The Geopolitics Behind the Routes Data Travel: A Case Study of Iran,” *Journal of Cybersecurity*, vol. 7, no. 1 (2021): p. 8.

[6] Farzan Sabet and Roozbeh Safshekan, “Soft War: A New Episode in the Old Conflicts Between Iran and the United States,” *Iran Media Program*, November 2013, p. 18, https://bit.ly/3L9RoCg.

[7] “Iran Orders Bandwidth Expansion to Boost Internet Speed,” *PressTV*, February 23, 2022, https://bit.ly/3KUwHt5.

Council, in addition to hiring proxy groups to conduct cyber operations.[8] For instance, the Iranian Cyber Police, known as the FATA, monitors Iranian online activities, which leads to the prosecution of alleged online dissidents and shutting down websites deemed un-Islamic and vulgar. Meanwhile, the Committee for Determining Offensive Contents controls censorship policies, updating lists of censored websites, whereas the IRGC Electronic Warfare and Cyber Defense Organization known as the Iran Cyber Army prevents cyber-attacks and implements counterattacks globally. In concert with these internet government agencies and proxies, telecommunications companies and actors such as the Mobile Telecommunication Company of Iran are another integral part of the infrastructure of internet censorship especially with suppressing information spread through communication technologies and mobile devices while acting under TCI, which altogether control 57.4 million internet users out of more than 82 million people living in Iran.[9]

By overly bureaucratizing information controls in Iran, Iranian citizens experience extreme technical and regulatory measures through the telecommunications industry, as well as NIN. NIN even affords users the ability to access cyberspace. Since its inception, NIN sought to fully substitute the public internet with an intranet, thereby cutting off Iranian citizens from the global internet as part of the government's soft war and soft power strategy domestically and globally. Originally, officials noted that cutting Iran off would paralyze not only many Iranian institutions but also hinder the state's economy through a complicated process. Similar to the Great Firewall of China, the government opted that NIN would continue its long-term strategy of controlling the media and online communications of its citizens through a "closed network" in 2006.[10] Alongside NIN, several other governmental bureaucracies and proxies maintain this "closed network" otherwise known as "halal internet" through tools and monitoring systems to manage citizens' use of cyberspace. The "halal internet" was introduced in 2011 to promote an advanced version of the national intranet, essentially arguing that citizens' use of the World Wide Web constricted their freedom and therefore required internet filtration and content control.[11] Launched by Ali Agha-Mohammadi, a former deputy vice president of economic affairs and member of the Parliament of Iran, the "halal internet" also consisted of a master plan to further develop internet and communication technologies alongside internet censorship by establishing a completely walled and closed off system. Essentially, the "halal internet" presented itself as an opportunity of the political elite to contest power over Iranian internet users in cyberspace. Implementing a "halal internet" can thus be ascribed as a soft war response to the 2009 Iranian Green Movement, which consisted of popular protests against the re-election of Mahmoud Ahmadinejad as President of Iran. The restrictive nature of the Iranian censorship policies further called in to question internet freedom in Iran.

[8] "Iranian Offensive Cyber Attack Capabilities," *Congressional Research Service*, January 13, 2020, https://bit.ly/37DjWWl.

[9] "Iran: Tightening the Net 2020: After Blood and Shutdowns," *ARTICLE 19*, September 2020, p.13, https://bit.ly/3OJ3zIC.

[10] "10 Things You Should Know About Iran's Multi-Billion Dollar National Internet Project," *Center for Human Rights in Iran*, October 13, 2016, https://bit.ly/3Lao5zG.

[11] Farid Shirazi, "Interrogating Iran's Restricted Public Cloud: An Actor Network Theory Perspective," *Telematics and Informatics*, vol. 31, no. 2 (2014): p. 1.

A Push for Internet Information Controls During Protests

On June 12, 2009, Mahmoud Ahmadinejad was re-elected with 63% of the vote.[12] The Iranian government responded by temporarily shutting down the internet during the announcement of election results on 13 June. Iranians, however, rejected the incumbent President Ahmadinejad, reporting irregularities with voting. As a response, some citizens implemented DDoS attacks – a disruption of online traffic to a specifically targeted network – aimed at sites that supported Ahmadinejad, and to mobilize mass protests in Tehran.[13] Popular unrest thus galvanized, which included citizens taking to the streets while also bypassing the filternet using anti-censorship tools like virtual private networks (VPNs). In sharing the events on social media sites like Facebook and Twitter, they could document their lives and produce discourse on their political situation with peers. VPNs were and are a necessary means to have full access to cyberspace beyond the limited confines of Iranian Cyberspace. This is by and large because the Iranian government owns the internet servers, meaning unless a VPN is used, or rather a way to cloak online activity through an encrypted connection, the government sees every internet address a citizen interacts with in cyberspace. During the Green Revolution, the state sought to control the cultural narrative and tackle the spread of information across Iranian cyberspace from the opposition by disrupting internet access and landline connections as a soft war strategy to prohibit VPN use and information spread. In addition to internet connection throttling (or slowing down internet speeds), the government crackdown against protestors also consisted of military violence, torture, arrests, swiping memory cards, and destroying computers.

In addition to internet disruption, the SMS system was significantly hindered by authorities so that citizens would not be able to text anti-government sentiments and further organize the opposition. As a response to citizens' counter-political engagement, the government's so-called "halal internet" had sought to quell any dissent, including values outside of the norms and political preferences of the government as a soft power tactic. The "halal internet" tactic also fell under the soft war agenda of censorship in part to put into motion the quelling of future post-election protests, and to assure that Iranians would not succumb to either outside or inside anti-government perspectives. This is evidenced by Ayatollah Khamenei stating, "Today, the country's priority is to fight the enemy's soft war," five months after the 2009 elections, and thus further cemented the importance of soft war in Iran.[14] Cyber political measures therefore became an imperative goal after 2009, leading to establishment of the centralized agency Supreme Council for Cyberspace by Ayatollah Khamenei in 2012. The Supreme Council for Cyberspace controls the following government bodies responsible for censorship: the Committee for Determining Offensive Contents, FATA, and the Cyber Defense Command.[15] Together, these entities along with several other institutions and proxies make up a

[12] Nergar Motaahedeh, *#iranelection: Hashtag Solidarity and the Transformation of Online Life* (Stanford, California: Stanford Briefs, 2015), p. 2.

[13] Noah Shachtman, "Activists Launch Hack Attacks on Tehran Regime," *Wired*, June 15, 2009, https://bit.ly/3KbZUPX.

[14] "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," *ARTICLE 19*, 2017, p. 2, https://bit.ly/3K9ehob.

[15] Simurgh Aryan, Homa Aryan, and J. Alex Halderman, "Internet Censorship in Iran: A First Look," *FOCI 13*, 2013, p. 1, https://bit.ly/36FcWaT.

more complicated infrastructure to further slowdown the internet of home users through the implementation of DNS hijacking and redirection, keyword filtering, and throttling.

Intentionally reducing internet speeds continued as a central tactic for internet censorship during the 2013 presidential election, with the intent to preserve calm, or in other words, prevent protest.[16] Since the use of VPNs affords access to servers outside of Iran, blocking them continued to be a countermeasure to not only prevent politically offensive and deemed criminal or vulgar behavior, but complete control of content to preserve the state narrative. Iranian authorities censored the public further to prevent social network-inspired onslaughts, and thus, email access was excruciatingly challenging during the 2013 presidential elections. Indeed, citizens aimed to share multimedia content across communication channels, and receive outside news content, and so, jamming and blocking communication effectively rendered VPNs useless and prevented freedom of expression.[17] To further achieve soft war during the election period, authorities extensively used DDoS attacks as a method to prevent access to websites and at the same time, phishing reporters and activities using surveillance software or viruses.[18] Additionally, SMS messages were heavily filtered for specific political slogans that contained names like Esfandiar Rahim Mashaei so that citizens would not be able to spread information to collectively organize.[19]

Outside of election cycles, Iranians have also protested the government when facing economic issues. In late 2017 through early 2018, citizens protested high prices of goods, and the government responded by temporarily banning Telegram and Instagram, as these platforms were central to organizing gatherings and sharing digital media on state-sanctioned violence and death during protests.[20] Linked to financial disarray in Iran under egregious US maximum pressure policies, the weight of foreign sanctions caused Iran's currency to take a severe plunge leading to escalating oil prices. By 2019, fuel prices skyrocketed in Iran, leading to citizen dissent and the government's repressive measures of violent crackdowns and an internet blackout, known as "Bloody November."[21] Throughout the protests, millions of Iranians were disconnected from the internet by the government.[22] While facing harsh sanctions, citizens experienced the state's first leveraging of Border Gateway Protocol, which effectively afforded the Iranian government the ability to operate its own domestic autonomous network, as planned since 2006, which effectively censors and leverages connectivity.[23] By 2021, citizens continued to face onslaughts by the authorities with blackouts relating to water

[16] Golnaz Esfandiari, "Iran Admits Throttling Internet to 'Preserve Calm' During Election," *Radio Free Europe Radio Liberty*, June 26, 2013, https://bit.ly/3MtF3ZM.

[17] Collin Anderson, "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran," *arXiv*, June 18, 2013, p. 1, https://bit.ly/3xOZBbm.

[18] James Ball and Saeed Kamali Dehghan, "Iran Accused of Using Online Censorship and Hacking to Sway Presidential Poll," *The Guardian*, May 31, 2013, https://bit.ly/39ezMar.

[19] "Freedom on the Net 2013 – Iran," *Freedom House*, October 3, 2013, https://bit.ly/3KePXkK.

[20] Simin Kargar, "Iran's National Information Network: Faster Speeds, but at What Cost?" *Internet Monitor*, February 21, 2018, https://bit.ly/3LdNOah.

[21] "Iran: No Justice for Bloody 2019 Crackdown, No Accountability, Threats Against Families," *Human Rights Watch*, November 17, 2020, https://bit.ly/3k7PRkd.

[22] "Iran: Tightening the Net 2020: After Blood and Shutdowns," *ARTICLE 19*, September 2020, p. 12, https://bit.ly/3OJ3zIC.

[23] Salamatian et al., "The Geopolitics Behind the Routes Data Travel," p. 1.

shortage protests, which further galvanized the government to up the ante on repressive internet measures to prevent access to global cyberspace.

"Bill for Protection of Cyberspace Users"

Citizens face ongoing efforts by the Islamic Republic of Iran to further censor and filter the internet through legislation, which consequently undermines human rights to freedom of expression and secure online privacy in the name of soft war and soft power. Iranian lawmakers have put significant stress on the parliament's regulations department to pass the "Bill for Protection of Cyberspace Users," beginning in 2021. Under Article 11, government authorities and institutions would have access to private information through monitoring of its users, while Article 15 would categorize users based on their job description and specify how much internet access they have depending on their skill level.[24] The "Bill for Protection of Cyberspace Users" would further regulate and prevent access to online information depending on the level of one's permit issued by the government. Although popular global services and websites like YouTube and Twitter are supposedly not accessible and thus severely restricted, VPNs have been a productive countermeasure against the Iranian government. However, the bill would effectively criminalize the distribution and use of VPNs through imprisonment and block the use of Instagram, resulting in citizens being isolated internationally, further persecuted, and subjected to a hostile online environment. President Ebrahim Raisi, as well as other top officials, have talked about creating "legal VPNs" in the case of VPN criminalization.[25] Fortunately, decision makers overturned the bill in February 2022, although pressures are still mounting to have the bill passed. While internet speeds and content access will be deeply impacted, local businesses in Iran that use Instagram as a promotion technique will experience financial deficits, a threat to Iran's booming e-commerce since the onset of COVID-19.[26] Iranian internet users continue to experience extensive throttling of internet speeds, oftentimes at random.

Iranian Cyberspace soft war and information controls has led to weaponized propaganda and therefore has had real-world impact on citizens' access to global cyberspace during and outside times of protest. While the Iranian government uses countermeasures enacted by its sophisticated censorship infrastructure to maintain the state's narratives and prevent the spread of information among citizens, Iranian internet users continue to find workarounds to gain access to popular websites, social media, and even applications like Telegram and WhatsApp, which are currently censored. Minor impediments such as internet filtering have been easily passable by Iranian citizens using VPNs and proxy servers, yet with the increased sophistication of state countermeasures, citizen tactics have also amplified. For instance, one Android cell phone application called Nahoft,

[24] "The Full Text of the Latest Version for the 'Plan of Cyberspace Service Regulation System' (protection): The Flaws Remain," *Shargh Daily*, February 19, 2022, https://bit.ly/38eDZdB.

[25] Sayeh Isfahani, "The Internet 'Protection Bill' Will Hurt All Iranians, But the Queer Community Will Have the Most to Lose," *Atlantic Council*, April 12, 2022, https://bit.ly/3EFhjiV.

[26] Layla Hashemi, "Threats to Iranian Instagram: Analyzing Iran's Internet Landscape," *Fikra Forum*, November 24, 2021, https://bit.ly/3k9nt17.

meaning “hidden” in Persian, allows users to send encrypted messages to others over applications like Telegram and WhatsApp, and Nahoft will translate encoded messages, even if access to global cyberspace is prohibited in Iran, especially if the application is already downloaded onto the Android phone.[27] Although the territorialization of Iranian Cyberspace will likely remain a geopolitical cyber strategy, Iranian citizens will continue to find ways to fully access global cyberspace despite the complexity of Iranian authorities’ initiatives as online communication is vital during heightened suppression. For the time being, Iranians can rely on evasion techniques to avoid state persecution that seeks to monitor and arrest those who criticize the establishment.

[27] Lily Hay Newman, “A New App Helps Iranians Hide Messages in Plain Sight,” *Wired*, September 17, 2021, https://bit.ly/3rM8Mp7/.