ANALYSIS

PEACE AND SECURITY

THE INTERNET IN THE WOMEN, LIFE, FREEDOM ERA

Iran's Progress in Censorship and Surveillance – and Options for European Policymakers

Miaan Group
June 2024

This report discusses Iran's National Information Network (NIN), a system designed to control and surveil internet usage, which played a central role in suppressing the »Women, Life, Freedom« movement.

It highlights the government's efforts to enforce political, social, and moral rules online, especially regarding women, and the impact of sanctions on internet access.

The report concludes with policy recommendations for improving internet freedom and security in Iran.

FRIEDRICH EBERT STIFTUNG

PEACE AND SECURITY

THE INTERNET IN THE WOMEN, LIFE, FREEDOM ERA

Iran's Progress in Censorship and Surveillance – and Options for European Policymakers

Content

1

INTRODUCTION

The "Women, Life, Freedom" protest movement in Iran, catalyzed by the tragic death of Mahsa Jina Amini, a young Kurdish-Iranian woman[1], in the custody of Iran's morality police on September 16, 2022, marked a significant shift in the country's socio-political landscape. Anti-government social mobilization reached historic levels, with months of sizable protests taking place in over 100 cities and all 32 provinces in the country.[2] The movement was organized through various online forums and galvanized through sharing videos of police violence against protestors on platforms such as Instagram and Telegram.

As Amini's arrest came after she allegedly failed to comply with the Islamic Republic's hijab mandate, women and women's bodies played a central role in the protests, particularly in their early days. Women began openly resisting hijab laws in public and posting videos of themselves doing so.

The Iranian government responded to the "Women, Life, Freedom" movement with an aggressive crackdown, which extended to online spaces. Initially, authorities aimed to quell the protests and social mobilization through a range of censorship tactics, such as localized and mobile-only internet blackouts, digital curfews, and aggressive attacks against VPN services. But soon after, policymakers looked for ways to intensify their information controls. In particular, the Islamic Republic began developing a more sophisticated surveillance framework, hoping to consolidate its control over the population further, maintain social order, and enforce its religious and ideological mandates.

The evolution of Iran's internet policies and information control can generally be divided into three eras. Each era emerged in response to a significant social uprising, shaping the government's strategy for digital oversight and control.

The first era began after the 2009 contested presidential elections, which led to months of large-scale protests known as the "Green Movement." This wave of dissent marked the first instance in which Iranians heavily leveraged the internet as a tool for mobilization and communication, even giving rise to the term "Twitter revolution"[3] among some commentators. Iranian leaders soon saw the need for a comprehensive approach to information controls, and by January 2011, Iran's Fifth Development Plan had set the creation of the National Information Network (NIN) in motion. While online censorship initiatives had already started before 2009, it was after the "Green Movement" that such measures were formalized and intensified. This period also witnessed the enactment of cybercrime laws and increased efforts to provide clear cyber policies to manage information flows and curb dissent.

The NIN, an amalgamation of regulations, market incentives, infrastructure, and technologies, is a localization project aimed at isolating Iranian users from the global internet. By restricting user's access to information and services based outside the country, the Islamic Republic gives itself maximum control over content, connectivity, and private user data. This localization effort, in part, has given rise to a vast expansion of public and private initiatives to develop Iran-based digital infrastructure, tools, services, and content. Iran's localization plan has also been inadvertently accelerated by US extra-territorial economic sanctions that have forced Iranian companies and users to pull their websites, services, and data off international cloud providers and move them onto Iran-based servers.

The second era catalyzing the NIN project started in November 2019, when a country-wide uprising against economic and political injustice occurred after a sudden fuel subsidy cut. The state's response, marked by severe crackdowns, detentions, and violence, led to the death of at least 300 demonstrators, according to Amnesty International, and a week-long internet blackout.[4] The shutdown resulted in Iranians

1 "Death of Jina Mahsa Amini," Britannica, April 25, 2024, https://www.britannica.com/biography/death-of-Jina-Mahsa-Amini.

2 "Woman, life, freedom; Comprehensive report of 20 days of protest across Iran." HRANA, October 12, 2022, https://www.en-hrana.org/woman-life-freedom-comprehensive-report-of-20-days-of-protest-across-iran/?hilite=Woman+life+freedom%3B+Comprehensive+report.

3 "EDITORIAL: Iran's Twitter revolution," Washington Times, June 16, 2009, https://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/.

4 "Iran: Details released of 304 deaths during protests six months after security forces' killing spree," Amnesty International, May 20, 2020, https://www.amnesty.org/en/latest/news/2020/05/iran-details-released-of-304-deaths-during-protests-six-months-after-security-forces-killing-spree/#:~:text=Amnesty%20International%20has%20released%20details,on%2016%20and%2017%20November.

losing access to all international content and services, such as BBC Persian, Twitter, and WhatsApp, essentially isolating Iranians from the world and each other. This was the first instance in the world where such an extensive and prolonged internet shutdown had occurred.

However, just as significantly, the shutdown demonstrated the functionality of the NIN, as Iran's domestic content and services remained online and usable. In other words, while Iranians could not access international services, most could still go online to check their bank accounts, read the local news, order cars on ride-sharing apps, and so on.

What we are seeing in the NIN's third era, born out of the "Women, Life, Freedom" movement,[5] is an Islamic Republic leveraging this project to its full potential, employing a suite of regulations and digital instruments to build toward a hyper-surveillance regime that can detect and counter both online and offline forms of political and moral dissent and monitor the lifestyle choices of Iranians.

The "Bill to Support the Culture of Chastity and Hijab," for example, introduced into the parliament in August 2023, would impose harsh penalties for non-adherence to compulsory hijab standards in physical and digital spaces and create a set of responsibilities for state agencies in enforcing those standards.[6]

Authorities are also developing various technologies, such as the Nazer application[7] for reporting hijab violations and facial recognition systems designed to monitor compliance with modesty laws.[8] Furthermore, the Islamic Republic's most ambitious new effort is to use the NIN infrastructure and platforms to collect big data and create "lifestyle" profiles of Iranians.[9]

In the face of these challenges, Iranian civil society and internet users have shown remarkable resilience and creativity in challenging the government's digital repression. They have developed and used circumvention tools to bypass online censorship and campaigned against legislation that would increase the government's authority over user data. When possible, Iranian users have largely resisted using NIN tools and services, such as Iran-based messaging apps, social media, and other domestic alternatives for online services ranging from navigation apps to email and search engines, preferring instead to use international ones even after those international ones are blocked

Against this backdrop, this report investigates how internet access and digital rights in Iran are shaped by various factors, such as technology, government policy, and sanctions, and offers policy recommendations for improving internet freedom and security. The report covers five main topics:

1. The development and implementation of the domestic intranet, the NIN.

2. The state of internet access and censorship in Iran and the challenges for internet users.

3. The government's increasing efforts to develop a hyper-surveillance regime to enforce its political, social, and moral rules, especially as they pertain to women in public and digital spaces.

4. The effects of US and EU sanctions on internet access in Iran.

5. Policy recommendations for improving internet access and freedom in Iran, addressing the needs and concerns of various stakeholders.

---

5 "Woman, Life, Freedom: A Roundup of the State of Digital Rights in Iran During the Protests," Melody Kazemi, Filterwatch, January 27, 2023, https://filter.watch/en/2023/01/27/women-life-freedom-the-state-of-digital-rights-during-the-protests/.

6 "Explained: What is Iran's Controversial Hijab and Chastity Law," Pejman Tavahori, IranWire, March 13, 2024, https://iranwire.com/en/women/126365-explained-what-is-irans-controversial-hijab-and-chastity-law/.

7 "Nazer App: How Iran is Using Technology to Suppress Women's Rights," Filterwatch, January 5, 2024, https://filter.watch/en/2024/01/05/nazer-app-how-iran-is-using-technology-to-suppress-womens-rights/.

8 "Facial recognition results," Filterwatch, https://filter.watch/en/?s=facial+recognition.

9 "Iran's 'People's Lifestyle Assessment System': A New Surveillance Threat," Louis Shakibi, December 14, 2023, https://filter.watch/en/2023/12/14/irans-peoples-lifestyle-assessment-system-a-new-surveillance-threat/.

2

THE RISE OF THE NATIONAL INFORMATION NETWORK

In 2006, then-Telecommunications Minister Mohammad Soleymani announced that Iran would begin constructing a "National Information Network" (NIN) in two to three years. After the 2009 Green Movement, in which the internet was used to mobilize mass protests, the Islamic Republic's perspective on the internet changed tremendously, and the NIN was recast as a national security project as much as a telecommunications infrastructure development project.

Iran's NIN was largely inspired by the by the approach of other countries to the internet, which promoted economic development within the context of strict information controls. The NIN is an amalgamation of laws and regulations, infrastructure, technologies, market incentives, and contents designed to create a localized alternative to the worldwide web.

The NIN project is a double-edged sword. While it can be credited for expanding Iranian telecommunication infrastructure and providing valuable baseline internet access for many Iranians, it simultaneously creates a broad-ranging system to curb free, safe access to the internet.

NIN – AN ARCHITECTURE BUILT FOR CONTROL

In 2011, the legislation of Iran's Fifth Development Plan formally characterized the NIN as an IP-based framework, complete with the necessary switches, routers, and data centers to direct online traffic domestically. This setup was intended to establish a secure, private, and nationally-contained intranet.

The Supreme Council for Cyberspace (SCC), the country's highest internet regulatory body, further refined the design and requirements of the NIN in 2016 with the enactment of the "Explanation of the Requirements of the National Information Network." This document refined the design and requirements of the NIN, providing further details and clarifying and enhancing the specifications of the NIN. The SCC outlined the NIN as a communication infrastructure with completely independent domestic management, capable of offering various types of content and nationwide communication services and providing secure services, including encryption and digital signature, to all users.

According to the SCC's "Comprehensive Plan and Architecture of the National Information Network" document in 2020, the architecture of the NIN consists of three layers: infrastructure, services, and content, each further divided into two sublayers. This structure ensures a comprehensive and organized approach to managing the network's various components.

- **The infrastructure layer** encompasses communication and information infrastructure sublayers. The communication infrastructure sublayer includes various mediums, such as wireless, wired, cable, and fiber, alongside the provision of communication services. The information infrastructure sublayer focuses on data centers, computing resources, and data storage solutions.

- **The services layer** consists of basic services with essential tools and application services. Basic services and essential tools comprise cloud infrastructure services, operating systems, search engines, basic navigation and map services, email, messaging and social networks, public key infrastructure with digital certificates, digital service platforms, repositories, libraries, and essential APIs. Application services encompass e-government services, audio and video services, advanced navigation, smart home products, data analysis services, food delivery apps, and more.

- Atop these two layers is **the content layer**, divided into content format and content application sublayers. This layer includes games and entertainment, government data, encyclopedias and publications, augmented reality content, virtual reality content, image and video content, as well as audio and music content.

With the Seventh Development Bill, enacted on May 20, 2023, the ICT Ministry aims to connect 20 million households to the NIN through fiber optic cables by 2026, near-universal coverage, including all urban areas and 99% of villages with over 20 households.[10]

10 "The Iranian government's use of technology to control and surveil its citizens," Louis Shakibi, Filterwatch, October 12, 2023, https://filter.watch/en/2023/10/12/the-iranian-governments-use-of-technology-to-control-and-surveil-its-citizens/.

The NIN was constructed on top of the pre-existing infrastructure that links Iran to the global internet through two primary secure border gateways with specific ports for external connection. The Infrastructure Telecommunication Company (ITC) has the sole authority to import and disseminate internet bandwidth within Iran. Acting as the intermediary, the ITC acquires international internet bandwidth and distributes it to local Internet Service Providers (ISPs). Meanwhile, the Institute for Research in Fundamental Sciences (IPM) is tasked with allocating bandwidth predominantly to educational institutions and government agencies. Additionally, the IPM is pivotal in administrating top-level domains such as .ir and .iran.

This centralized gateway system simplifies the process for the authorities to isolate the NIN from the international internet, allowing them to swiftly disconnect the domestic network from the outside world when deemed necessary.

In May 2024, Iranian lawmakers reintroduced a controversial bill proposal, the "User Protection Bill,"[11] into parliament's agenda.[12] One of the main goals of this bill is to hand over control of the internet's entry/exit gateways in Iran to the military, which would facilitate extensive and extrajudicial surveillance of users at the gateways. The bill had been floating around the parliament since 2021 and twice came near a vote. However, digital rights advocates in Iran raised grave concerns about the bill's impact on internet freedom and privacy, sparking an enormous public outcry, which effectively forced lawmakers to abandon the legislative efforts. Yet, in May 2024, MP Ahmad Rastineh stated that the newly reintroduced bill, having met certain procedural requirements, could be swiftly ratified with just ten minutes of discussion on the parliamentary floor, effectively bypassing a general assembly vote and enabling it to be directly enacted.[13]

DOMESTIC SERVICES AND PLATFORMS

A key aspect of the NIN is the development, support, and mandated use of domestic platforms. These platforms serve as alternatives to international basic services, online tools, apps, and platforms, ranging from navigation apps to national email to search engines. While authorities regularly tout the economic benefits of local services and app markets, this localization strategy is also a pivotal part of the state's approach to information control.[14] Local alternatives are hosted within the country, comply with the laws of the Islamic Republic of Iran, and have infrastructural dependencies on the government. In effect, authorities can regulate and censor content on these platforms while also having access to user data.

At the same time, authorities block countless international websites and applications. These include navigation apps like Waze, major social media and messaging platforms like Instagram and Telegram, various news outlets like BBC Persian, and application stores like Google Play. These platforms can only be accessed using Virtual Private Networks (VPNs), making the local alternatives much easier to access.

The government also employs a range of other policies to drive users towards the NIN platform and websites. By law, traffic within the NIN costs far less than traffic to the global internet, forcing consumers to make pocketbook decisions about whether to use international platforms.[15]

To incentivize the private sector to use and operate on domestic platforms, the government also offers businesses special tax breaks, bank loans[16], placement in science and technology parks, and a share in traffic sales revenue for content producers on domestic platforms.[17]

Since 2012, the Iranian government has implemented policies that require the use of locally developed messaging apps for various online activities. This includes transactions in banking, accessing e-government services, and the enrollment process for educational institutions. "Domestic social messengers" in this context are defined as those with over 50% Iranian ownership and exclusively hosted within the country. Examples include Bale, Eitaa, Rubika, and Soroush.[18] These regulations effectively compel most Iranians to install and use these domestic messengers to some degree. Moreover, the e-government portals themselves serve as massive databases of user data that authorities can easily access and cross-reference.

By creating a wide array of localized online services and content, the Islamic Republic has also eased the pain of internet shutdowns. During major disruptions or shutdowns, access to the global internet is cut, but the local alternatives remain online. In other words, a functional NIN minimizes the neg-

11 "Investigative Report: Answering Six Questions About the Protection Plan in Simple Language," Filterwatch, April 14, 2022, https://filter.watch/fa/2022/04/14/answer-six-questions-about-the-user-protection-plan-in-simple-language/.

12 "The 'Protection Plan' returns to the Parliament's agenda!" Khabar Online, May 12, 2024, https://www.khabaronline.ir/news/1905572/.

13 "Protection Plan Waiting for Parliament's Minute," Hamshahri Online, https://hammihanonline.ir/%D8%A8%D8%AE%D8%B4-%D8%B3%DB%8C%D8%A7%D8%B3%D8%AA-18/16083-%D8%B7%D8%B1%D8%AD-%D8%B5%DB%8C%D8%A7%D9%86%D8%AA-%D9%85%D9%86%D8%AA%D8%B8%D8%B1-%D8%AF%D9%82%DB%8C%D9%82%D9%87-%D9%88%D9%82%D8%AA-%D9%85%D8%AC%D9%84%D8%B3.

14 "Ana reports; A golden opportunity for the digital economy / What has the government done to support online businesses?" Ana, May 15, 2024, https://ana.ir/fa/news/910849/.

15 "Government Accelerates Localization In Response To Financial Cost Of Internet Shutdowns," Filterwatch, January 26, 2023, https://filter.watch/en/2023/01/26/policy-monitor-december-2022/.

16 "Granting 500 million Toman facilities to businesses active on domestic platforms," ISNA, May 7, 2024, https://www.isna.ir/news/1403021813006/.

17 "The Islamic Republic's Vision for Domestic Platforms and Enhanced Regulation of Cyberspace," Louis Shikabi, Filterwatch, September 20, 2023, https://filter.watch/en/2023/09/20/policy-moniotor-july-2023/.

18 "Text of the Social Media Messaging Regulation Plan," ISNA, November 19, 2018, https://www.isna.ir/news/97082813960/.

Figure 1
"Relatively Successful Test of the 'National Internet,'"

Source: Jam-e Jam Newspaper, November 20, 2019; https://jamejamdaily.ir/?nid=5529&type=0

ative impact of shutdowns on Iranian users and businesses and thus lowers the government's social, political, and economic costs.

Of note, after the nationwide internet shutdown in 2019, Mohammad-Javad Azari Jahromi published a video stating that banking and online services operated on the NIN were still functional.[19] For the then-minister of communications, this was proof of the NIN's functionality.

WAR AGAINST INTERNATIONAL BANDWIDTH

Part and parcel to the government's promotion of NIN content, tools, and services is an effort to limit international bandwidth. As mentioned above, accessing the global internet is notably more expensive for users than accessing the NIN. The "Comprehensive Plan and Architecture of the National Information Network," approved on October 7, 2020, by the SCC, contained more than 30 objectives for the "Operational Goals of the National Information Network."[20] These objectives included "allocating a 70 to 30 percent traffic share ratio for domestic versus foreign services" and "setting tariffs at two to three times higher for accessing the global network compared to the domestic content and services of the NIN." Based on a directive from the Regulatory Authority issued in December 2021, the fixed and mobile internet tariff rates increased by 34%.[21] According to officials, this price hike applies only to international internet traffic and does not affect domestic traffic.

Figures related to the country's inbound internet bandwidth have not been officially published. In late 2021, reports indicated that internet companies blamed the reduction in speed and quality of their services on insufficient bandwidth imports since President Ebrahim Raisi's administration started.[22] They cited this shortage as the reason for the declining

19 "Azari Jahromi's explanation about the National Information Network and the one-week global network outage: I apologize for the internet outage on my part," Khabar Online, November 23, 2019, https://www.khabaronline.ir/news/1323957.

20 "NATIONAL INFORMATION NETWORK MACRO-PLAN AND ARCHITECTURE RESOLUTION," Filterwatch, https://filter.watch/en/docs/national-information-network-macro-plan-and-architecture-resolution/.

21 "Blocking Access to the Global Internet Through Economic Pressure," Filterwatch, February 16, 2024, https://filter.watch/en/2024/02/26/policy-monitor-jan-2024/.

22 "Infrastructure CEO: We have no problem with bandwidth imports," Zoomit, February 6, 2022, https://www.zoomit.ir/tech-iran/379232-no-problem-importing-bandwidth/.

internet quality and speed in recent months. However, the Deputy Minister of Information at the time denied these claims.[23] In February 2024, Ladjevardi, the head of the Communication Regulatory Authority (CRA), stated that based on the recorded traffic volume, it can be concluded that the traffic is 5.5 terabits per second. It should be noted that Iran has a population of 88 million.[24]

In reality, limiting international traffic bandwidth and intentionally disrupting access are indirect censorship methods targeting websites not hosted within Iran.[25] Throttling internet speeds have been used to slow services and restrict information flow during critical events like protests. This tactic is now an official part of the government's cyber policy. These strategies discourage using services outside the NIN, steering users towards domestic platforms. By making international content slow, unreliable, and expensive, authorities limit exposure to diverse viewpoints and international communication apps and social media platforms that they cannot easily monitor.

---

23 "Policy Monitor – December 2021," Melody Kazemi, Filterwatch, January 17, 2022, https://filter.watch/en/2022/01/17/policy-monitor-december-2021/.

24 "Lajevardi stated; The increasing trend of bandwidth since the beginning of the thirteenth government," Mehr News, February 13, 2024, https://www.mehrnews.com/news/6023097/.

25 "New Steps Toward Traffic Localization," Amir Rashidi, Filterwatch, February 8, 2023, https://filter.watch/en/2023/02/08/jan-2023-new-steps-toward-traffic-localization/.

3

ACCESS TO THE INTERNET IN PRACTICE

The Iranian government employs various methods of censorship to control the online activities and expression of its citizens, especially during times of social and political unrest. These methods include filtering, shutdowns, and throttling. At the same time, Iranian internet users, technologists, and digital rights activists have resisted these censorship methods by developing and relying on VPNs, circumvention tools, and satellite technologies.

FILTERING AND CONTROL OVER CONTENT

Following the disputed presidential election of 2009 in Iran, a wave of citizens turned to social media to express their dissent and organize protests.[26] This led to the Iranian government's decision to ban Facebook and Twitter. Subsequently, the Computer Crimes Act was enacted in 2009, establishing the "Committee for Determining Instances of Criminal Content" online.[27] This committee's directives for the blocking or filtering of online content became mandatory for internet service providers.

Filtering is accomplished with two basic methods: blocking keywords in the domain name and blocking specific addresses. The rationale behind these censorship practices varies, encompassing objectives from upholding the Islamic Republic's moral standards to limiting access to information from disfavored sources such as foreign-based news channels, human rights websites, websites of political opposition groups, and others not aligned with the government's policies. Filtering policies have led to the permanent blocking of widely used social media platforms (i. e., Instagram) and international messaging applications (i. e., WhatsApp and Telegram).

During the peak of the Woman, Life, Freedom protest in September 2022, the Supreme National Security Council issued the order to block Instagram, the last major international social media platform that was not blocked and by far the most widely used platform in the country.[28] Instagram's filtering was very illustrative because, at the time, a sizable number of local businesses had been operating on Instagram, and they were adversely impacted by the move.[29] According to statistics provided by online market experts in Iran, of the estimated 630,000 Iranian vendors active on Instagram before it was blocked, only about 220,000 remained by December 2022.[30] In other words, within approximately three months, more than 400,000 businesses temporarily or permanently left Instagram, resulting in an estimated loss of around USD 190 million in e-commerce sales.

Instagram was also the leading platform Iranians were using to share information and videos about the protests and police misconduct. By blocking Instagram and many other platforms, authorities were seemingly looking to hide information and evidence of human rights violations, as well as hinder social mobilization through digital communication tools. The crackdown on VPNs, essential for accessing global news portals and social media sites and bypassing messaging restrictions, has drastically limited free internet access, as Iranians lack effective tools for circumvention.[31]

---

26 "EDITORIAL: Iran's Twitter revolution," The Washington Times, June 16, 2009, https://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/.

27 "Computer Crimes Act," Cyber Police, September 13, 2013, https://sherloc.unodc.org/cld/uploads/res/document/computer-crimes-act_html/Computer_Crimes_Act.pdf.

28 "Sardar Jalali: The filtering of Instagram and WhatsApp has been carried out by the order of the Supreme National Security Council." Donyay Eqtesad, October 31, 2022, https://donya-e-eqtesad.com/%D8%A8%D8%AE%D8%B4-%D8%B3%D8%A7%DB%8C%D8%AA-%D8%AE%D9%88%D8%A7%D9%86-62/3913115-%D9%81%DB%8C%D9%84%D8%AA%D8%B1-%D8%A7%DB%8C%D9%86%D8%B3%D8%AA%D8%A7%DA%AF%D8%B1%D8%A7%D9%85-%D9%88%D8%A7%D8%AA%D8%B3%D8%A7%D9%BE-%D8%A8%D9%87-%D8%AF%D8%B3%D8%AA%D9%88%D8%B1-%D8%B4%D9%88%D8%B1%D8%A7%DB%8C-%D8%B9%D8%A7%D9%84%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D9%85%D9%84%DB%8C-%D8%A7%D9%86%D8%AC%D8%A7%D9%85-%D8%B4%D8%AF%D9%87-%D8%A7%D8%B3%D8%AA.

29 "Irreparable Damage to the Digital Economy caused by Government Deployed Internet Shutdowns and Online Censorship," Louis Shakibi, August 10, 2023, https://filter.watch/en/2023/08/10/irreparable-damage-to-the-digital-economy-because-of-to-internet-shutdown-and-online-censorship/

30 "Irreparable Damage to the Digital Economy caused by Government Deployed Internet Shutdowns and Online Censorship," Louis Shakibi, August 10, 2023, https://filter.watch/en/2023/08/10/irreparable-damage-to-the-digital-economy-because-of-to-internet-shutdown-and-online-censorship/

31 "Iran Technology; The Ministry of Communications was tasked with identifying and disabling VPNs." January 4, 2023, https://digiato.com/article/2023/01/04/ministry-communications-block-vpn-access.

SHUTTING DOWN THE INTERNET AS "CRISIS MANAGEMENT"

Since 2009, Iran has used internet policy as a tool for national security and social control. Alongside blocking and filtering content, the Iranian government has pioneered a number of restrictive methods designed to limit internet access, particularly during times of social and political unrest, most famously total internet shutdowns.[32] As mentioned, the growth of the NIN has made it less costly for Iranian authorities to shut down the internet, as domestic services can continue running isolated from the international internet.

During the November 2019 internet blackout, which resulted from the National Security Council ordering a nationwide internet shutdown that lasted a week, all access to international connections and services was effectively blocked. During this period, authorities violently clamped down on demonstrations, resulting in at least 300 protesters killed.[33] The shutdown demonstrated the government's information control capacity and marked the operational beginning of the NIN as an independent digital ecosystem. Despite the blackout, access to domestic services like online banking, rideshare apps, and online shopping was maintained.

During the Woman, Life, Freedom protests, the authorities demonstrated a refined and highly tailored approach to shutdowns. After the protests began on September 16, 2022, internet shutdowns were first observed that evening. With protests often peaking at night, the imposition of evening shutdowns, starting around 4 PM local time, became a recurring pattern referred to as a "digital curfew."

During protests in Sistan and Baluchistan, Khuzestan, and Tehran in 2020, 2021, and early 2022, authorities relied on localized shutdowns.[34] Women, Life, Freedom protests met a similar fate, with shutdowns happening at the level of provinces, cities, and even neighborhoods, effectively only targeting areas where protests took place.

Another form of shutdown tailoring involves only blocking mobile data. These mobile-only shutdowns comprised the vast majority of shutdowns since 2019. They primarily affect internet connections from major cellular network providers such as Irancell, MCI, and RighTel. Mobile internet is a crucial aspect of internet access in Iran, with the Communications Regulatory Authority reporting over 100% mobile internet penetration, while fixed broadband access remains below 13%.[35]

It is understood that requests for internet shutdowns at the provincial level must be made by the respective governors and approved by the Interior Minister. When internet shutdowns are requested for several provinces at once, the President must approve the action.

While Iranian officials claimed the shutdowns were successful, their economic repercussions have been significant, with examples including a record sell-off at the Tehran Stock Exchange, disrupted shipping, and currency exchange services halted.[36] Different estimates place the economic loss of the ten-day 2019 shutdown at USD 370 million[37], USD 611 million[38], or a staggering USD 1.5 billion[39], according to the former president of the Iran Chamber of Commerce, Mohsen Jalalpour.

During the Women, Life, Freedom protests, internet disruptions and shutdowns reportedly cost the Iranian economy USD 773 million in September 2022 alone.[40]

USERS RESPOND WITH VPNS, SATELLITE, AND CIRCUMVENTION

Despite the sweeping array of NIN information controls emerging over the last 15 years, the Iranian public has been rather successful at escaping the limits of the NIN and accessing the content, tools, and experiences they seek.[41] Most notably, the vast majority of Iranians turned to VPNs to bypass the pervasive state filtering of platforms, messaging

32 "IRAN AND THE INTERNET," IRANIAN DIGITAL INFLUENCE EFFORTS: GUERRILLA BROADCASTING FOR THE TWENTY-FIRST CENTURY, Jan. 1, 2020, pp. 11-14, Accessed on Jstor, https://www.jstor.org/stable/resrep24668.6.

33 "Iran: Details released of 304 deaths during protests six months after security forces' killing spree," Amnesty International, May 20, 2020, https://www.amnesty.org/en/latest/news/2020/05/iran-details-released-of-304-deaths-during-protests-six-months-after-security-forces-killing-spree/#:~:text=Amnesty%20International%20has%20released%20details,on%2016%20and%2017%20November.

34 "Internet Shutdown Trends in Iran: November 2019 to July 2021," Melody Kazemi, Filterwatch, September 3, 2021, https://filter.watch/en/2021/09/03/internet-shutdown-trends-in-iran-from-november-2019-to-july-2021/.

35 "The quarterly report of the Regulatory Authority shows; The penetration rate of fixed internet continues to decline," April 28, 2024, https://www.sharghdaily.com/%D8%A8%D8%AE%D8%B4-%D9%81%D9%86%D8%A7%D9%88%D8%B1%DB%8C-298/928401-%D9%85%DB%8C%D8%B2%D8%A7%D9%86-%D8%B6%D8%B1%DB%8C%D8%A8-%D9%86%D9%81%D9%88%D8%B0-%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AB%D8%A7%D8%A8%D8%AA-%D9%87%D9%85%DA%86%D9%86%D8%A7%D9%86-%DA%A9%D8%A7%D9%87%D8%B4%DB%8C-%D8%A7%D8%B3%D8%AA.

36 "Massive Iranian internet shutdown could be harbinger of something even darker to come, experts warn," Independent, November 30, 2019, https://www.independent.co.uk/news/world/middle-east/iran-internet-shutdown-protests-communications-tehran-a9226731.html.

37 "Massive Iranian internet shutdown could be harbinger of something even darker to come, experts warn," Independent, November 30, 2019, https://www.independent.co.uk/news/world/middle-east/iran-internet-shutdown-protests-communications-tehran-a9226731.html.

38 "Government Internet Shutdowns Have Cost $53 Billion Since 2019," Top10VPN, https://www.top10vpn.com/research/cost-of-internet-shutdowns/.

39 "The impact of the internet outage on the country's trade sector; Jalalpour: The internet outage caused a $1.5 billion loss to the economy," Khabar Online, November 23, 2019, https://www.khabaronline.ir/news/1323822/.

40 "Government Internet Shutdowns Have Cost $53 Billion Since 2019," Top10VPN, https://www.top10vpn.com/research/cost-of-internet-shutdowns/.

41 "Freedom on the Net 2023, Iran," Freedom House, https://freedomhouse.org/country/iran/freedom-net/2023.

apps, and websites. Indeed, VPNs have become an indispensable part of the daily digital life for most Iranians.

An August 2023 report by the Iran Parliamentary Commission of Industries noted that the volume of anonymous bandwidth on the international network, indicative of VPN use, had quintupled within a year. By November 2023, Iran's Parliament Research Center reported that 90% of internet users used VPNs.[42] The Research Center estimated that about 60 million Iranians had downloaded VPNs and other circumvention tools onto their devices. Psipone, Lanther, and Outlook are effectively free services dedicated to providing reliable unfiltered access to the internet for Iranians.

The Iranian government has employed various strategies to combat the use of circumvention tools. In addition to legal and judicial efforts that ban the distribution and use of VPNs, the government actively blocks these tools, particularly during periods of civil unrest, such as the Woman, Life, Freedom protests. During these periods, the authorities target the connection protocols of VPNs and block IP addresses associated with them[43], significantly hindering the availability of functional VPNs.[44]

In response to the Women, Life, Freedom protests, VPN providers were forced to rapidly adjust their protocols and invest in diversified ISPs and servers to throw off Iranian censors and meet public demand.[45] Additionally, over the last year and a half, technologists and VPN providers have been forced to develop new types of circumvention and VPNs that can, with varying levels of success, avoid government attacks and deal better with internet shutdowns.

On February 19, 2024, the Supreme Council of Cyberspace announced a new resolution entitled "Exploring Solutions to Increase the Share of Domestic Traffic and Counteract Anti-Censorship Tools."[46] Clause 6 of the resolution explicitly prohibits using internet filtering circumvention tools, including VPNs, which has raised public concern over the criminalization of these commonplace tools that are crucial for daily life. In addition, for years now, judicial and security authorities have been prosecuting producers and distributors of internet filtering circumvention tools and filing cases against them in judicial bodies.[47]

However, while authorities look to limit VPN usage, they are slowly introducing government-approved VPNs. This move towards government-approved VPNs is tied to a broader plan for tiered internet access that would balance internet restrictions with the need for global connectivity. This authorization-based system discriminates access, allowing individuals varying levels of internet content based on their social status, with journalists, for example, having limited access to certain sites like YouTube.

THE SATELLITE INTERNET CHALLENGE

In September 2022, at the peak of the Women, Life, Freedom protests and the government's internet shutdowns, satellite internet provider Starlink announced that it would make its transmission available inside Iran.[48] Some internet freedom activists soon advocated for Iranians to rely on Starlink and satellite technologies in general to avoid Iran's censorship and internet infrastructure in its totality.[49] In theory, the dishes offer easy access to uncensored, relatively fast, and reliable internet.

However, despite pervasive discussions around this alternative, the use of Starlink in Iran is not widespread, as the dishes are not legally available in the country and are costly. Even if some Iranians could afford the service, US sanctions have cut Iran's financial sector off from the world, making it almost impossible for Iranians to purchase the service. Still, advocates tell the Miaan Group that the number of Starlink dishes in the country totals between 4,000 and 5,000 as of May 2024, but many of them have not been put into operation. These devices are typically obtained through smugglers, and since their purchase and sale are illegal, their owners and operators are at risk of arrest.[50] Starlink services are also usually purchased by individuals outside of Iran for in-country dish owners.

Iranian authorities have vigorously responded to the challenge posed by Starlink. The use of Starlink satellite internet terminals is banned in Iran under the 1994 law prohibiting the use of satellite reception equipment, which states, "the

---

42 "Shocking parliamentary report on the statistics of VPN usage in Iran," Gadget News, November 17, 2023, https://gadgetnews.net/800682/vpn-using-statics-in-iran/.

43 "Technical multi-stakeholder report on Internet shutdowns: The case of Iran amid autumn 2022 protests," OONI, https://ooni.org/post/2022-iran-technical-multistakeholder-report/#circumvention-tools.

44 "Woman, Life, Freedom: A Roundup of the State of Digital Rights in Iran During the Protests," Filterwatch, January 27, 2023, https://filter.watch/en/2023/01/27/women-life-freedom-the-state-of-digital-rights-during-the-protests/.

45 "Fighting VPN criminalization should be Big Tech's top priority, activists say," Ars Technica, March 20, 2023, https://arstechnica.com/tech-policy/2023/03/fighting-vpn-criminalization-should-be-big-techs-top-priority-activists-say/.

46 "Solution to Increase the Share of Domestic Traffic," Filterwatch, https://filter.watch/en/wp-content/uploads/sites/2/2024/03/%D8%A8%D9%87%D9%85%D9%8629_1402-%D8%B1%D8%A7%D9%87%DA%A9%D8%A7%D8%B1-%D8%A7%D9%81%D8%B2%D8%A7%DB%8C%D8%B4-%D8%B3%D9%87%D9%85-%D8%AA%D8%B1%D8%A7%D9%81%DB%8C%DA%A9-%D8%AF%D8%A7%D8%AE%DB%8C.pdf.

47 "The use of VPNs is prohibited, but not criminalized," Filterwatch, March 4, 2024, https://filter.watch/en/2024/03/04/the-use-of-vpns-is-prohibited-but-not-criminalized/.

48 "Elon Musk says around 100 Starlinks now active in Iran," Reuters, December 27, 2022, https://www.reuters.com/technology/elon-musk-says-around-100-starlinks-now-active-iran-2022-12-26/.

49 "Satellite Internet Companies Could Help Break Authoritarianism," Pouria Nazemi, Scientific American, https://www.scientificamerican.com/article/satellite-internet-companies-could-help-break-authoritarianism/.

50 "Inside the Clandestine Efforts to Smuggle Starlink Internet Into Iran," Time, January 25, 2023, https://time.com/6249365/iran-elon-musk-starlink-protests/.

entry, distribution, and use of satellite reception equipment are forbidden except in cases specified by law." Additionally, a leaked confidential letter from Ali Bahadori Jahromi, spokesperson and head of the Information Council, to the Ministers of Economy and Industry, dated October 29, 2022, discusses banning the importation of Starlink satellite internet equipment due to their role in protests and facilitating communication among people.[51]

In October 2023, a news agency associated with the Islamic Revolutionary Guard Corps (IRGC) reported that national security agencies had intercepted a cargo of Starlink equipment, resulting in the arrest, prosecution, and forced confession of five individuals in Zahedan for receiving and operating this equipment.[52]

The Islamic Republic has also filed a complaint against Starlink with the International Telecommunication Union (ITU), protesting the operation of Starlink terminals within its territory without a license and arguing that such operations are unauthorized.[53] In October 2023, the ITU's Radio Regulations Board found that Starlink's operation within Iranian territory violated ITU regulations.[54] As of this writing, the complaint is still under review.

In contrast to Starlink, YAHSAT, another satellite internet provider, agreed in December 2023 to comply with Iran's territorial rules for landing rights.[55] As of May 2024, YAHSAT's licensing process was underway. Iran's Minister of ICT stated in December 2022 that international satellite internet operators that comply with Iran's laws and regulations are welcome, highlighting the need for connectivity in 3,000 villages across the country that still lack internet access.[56]

---

51 "The hidden war on internet access in Iran," Louis Shikabi, Filterwatch, https://filter.watch/en/2024/03/18/council-hacked-document-mar-2024/.

52 "Communication equipment of a spy service handed over to the security agency / 5 agents of the service were arrested," Tasnim, October 2, 2023, https://www.tasnimnews.com/fa/news/1402/07/10/2965033/.

53 "Submission by the Islamic Republic of Iran regarding the provision of Starlink satellite services in its territory," ITU, February 23, 2023, https://www.itu.int/md/R23-RRB23.1-C-0007/en.

54 "SUMMARY OF DECISIONS OF THE THE MEETING OF THE RADIO REGULATIONS BOARD," ITU, October 23-27, 2023, https://www.itu.int/dms_pub/itu-r/md/23/rrb23.3/c/R23-RRB23.3-C-0014!!PDF-E.pdf.

55 "Legal satellite internet will come to Iran," Fars News, https://fars-news.ir/news/14020927000220.

56 "The Minister of Communications' conditional welcome to Starlink's operation in Iran," ISNA, December 28, 2022, https://www.isna.ir/news/1401100703915/.

4

BUILDING TOWARDS A HYPER-SURVEILLANCE OF WOMEN, LIFESTYLES, AND PUBLIC MORALITY

As the Islamic Republic cements NIN in place, it has invested more into developing and deploying technologies to identify, monitor, control, and punish those who deviate from its religious, social, and political mandates. In fact, according to a former government insider, one of the original long-term goals of the NIN is to establish a hyper-surveillance regime.

Women and women's bodies, in particular, have become a central focus of Iran's recent surveillance technologies. Challenges to mandatory hijab seen within the Women, Life, Freedom movement only sharpened this focus. The emerging surveillance technologies include facial recognition and image processing, incident reporting apps, and a big-data Lifestyle Monitoring System. Officials aim to bolster these technologies through new laws and efforts to further control and create content for cyberspace. If successful, these technologies and policies, grounded in the NIN ecosystem, will facilitate a level of surveillance, censorship, and profiling yet unseen in Iran.

As articulated by various authorities, a primary objective of such measures is to demonstrate the government's firm commitment to enforcing hijab laws, moral compliance, and more. In the eyes of policymakers, they are building a digital surveillance and monitoring system that will allow them to enforce their laws and regulations strictly, many of which violate international human rights laws and ensure non-adherence to mandated hijab regulations, which will invariably be subject to legal penalties.[57]

FACIAL RECOGNITION AND IMAGE PROCESSING

Recent developments have made clear that the Iranian government has set its sights on attaining facial recognition technology. This technology drew controversy following claims by some Iranian officials, dating back to August 2022 that the government had the capability to identify women not adhering to mandatory hijab through facial recognition.[58] The issue took on new significance in the context of the Women, Life, Freedom movement, fueling more public concern.

In an interview with state media on April 8, 2023, Ahmadreza Radan, Chief Commander of the Iranian Police, announced that from March 20 to April 18, 2023, individuals violating hijab regulations were "identified using advanced technology and equipment, reprimanded, and referred to the judicial courts."[59]

Despite claims and speculation, the reality of the government's use of facial recognition surveillance practices remains unclear and is likely less sophisticated than officials purport. Evidence points to the continued use of traditional methods for monitoring and enforcement.[60] For example, in 2019, the Iranian police sent SMS warnings to drivers for wearing improper hijabs in their cars. However, men with long hair also received these messages. These false positives suggest a reliance on simpler, older camera technologies and maybe even manual review, as facial recognition would have pinpointed exactly who an alleged offender was.

Additionally, during the Women, Life, Freedom protests, authorities primarily used existing CCTV systems in public spaces to monitor and apprehend protesters, including women challenging the hijab law.[61] Arrest techniques often involved posting images on pro-government social

57 "Iran has launched a new crackdown on women defying its strict dress code," NBC News, May 9, 2024, https://www.nbcnews.com/news/world/iran-launches-crackdown-women-defying-hijab-dress-code-rcna151406.

58 "Secretary of the Headquarters for Promoting Virtue: With the help of facial recognition technology, we will fine individuals exhibiting unconventional behavior in public places." August 30, 2022, https://digiato.com/article/2022/08/30/financial-fine-facial-recognition-technology.

59 "Sardar Radan's final warning to women without hijabs | Starting Saturday, women without hijabs will first receive a warning; then they will be referred to the judiciary," Hamshahri Online, April 8, 2023, https://www.hamshahrionline.ir/news/752644/.

60 "Iranian government's digital control tactics are a sophisticated form of repression, says researcher," CBC News, February 20, 2023, https://www.cbc.ca/radio/spark/iranian-government-s-digital-control-tactics-are-a-sophisticated-form-of-repression-says-researcher-1.6743923.

61 "Surveillance and Secrecy: Examining Iran's Claims on the Use of Facial Recognition for Social Control," Filterwatch, May 28, 2023, https://filter.watch/en/2023/03/28/surveillance-and-secrecy-examining-irans-claims-on-the-use-of-facial-recognition-for-social-control//

media to solicit public assistance in identifying violators, further indicating a dependence on basic surveillance rather than cutting-edge technology.[62]

To date, the only evidence that the government is employing facial recognition, a sophisticated artificial intelligence technology, is that officials have themselves said so. It is possible that officials made such claims primarily to intimidate the public and maintain social control.

What Miaan's research has shown, however, is a clear attempt by the Islamic Republic to develop facial recognition technologies, as well as image processing software that can look at online images to see if they violate Iranian laws.[63]

Around 2015, several Iranian companies, including Yaftar and Niafam, began collaborating with the Iranian prosecutor's office to develop these technologies. Leaked communications between Yaftar and the prosecutor's office, for example, show that the company was specifically trying to develop the capacity to detect moral infractions, such as images of women without hijab or same-sex kissing.[64] However, as of this writing, little is known about how far these efforts have gotten.

Additionally, Iran seems to have tried to purchase cameras capable of facial recognition and other surveillance systems from foreign firms. According to media reports, from 2016 to 2018, the German company Bosch sold cameras to Iran capable of "intelligent tracking."[65] While Bosch denied that these cameras were equipped with facial recognition capabilities, they acknowledged that the Iranian state could potentially integrate software from another provider to enable facial image tracking using these cameras.

In addition, in December 2021, IPVM, a surveillance research group, reported on a contract between Tiandy, an Asian video surveillance company, and the IRGC and Iranian police. IPVM claimed that Tiandy cameras had been used by Sairan – a state-owned military electronics provider in Iran. Similar international firms such as Huawei and ZTE appear to be active inside Iran. Whether these companies have ever provided surveillance technologies or services to Iranian authorities is unclear. Reports do indicate that these companies have helped establish so-called "safe cities" and "smart cities" programs in Asian countries, which utilize artificial intelligence and various other technologies to monitor local populations. Iranian authorities regularly promote the idea of "smart cities."

Further complicating the landscape, a report by the research group Tehran Bureau indicates that other Asian firms, such as Huawei, have provided Iran with advanced surveillance technologies such as facial recognition, video surveillance, crowd monitoring, and communications interception. These deals often include comprehensive training programs to help Iran implement a "safe cities" model.

NAZER APP

An Android application called Nazer is used by the national police force of Iran to report vehicles with female occupants wearing "improper" hijab. In 2023 and 2024, authorities punished women for violating hijab mandates while driving by issuing fines and impounding their cars after being identified by law enforcement. Nazer aims to streamline this type of enforcement.

Nazer is a Persian word that means "supervisor" or "overseer." For now, the app can only be used for hijab violations. However, static analysis of its code reveals that with future updates, the app could also be used to report people for protesting, drinking alcohol, "cruising around" in vehicles, and other things the government deems criminal.

Figure 2
The Nazer App

62 "Identify the rioters," Gerdab, October 12, 2022, https://gerdab.ir/fa/news/33714/.

63 "Internet Oppressors: A Look at the Office of Iran's Attorney General and its Contractors," Filterwatch, September 14, 2023, https://filter.watch/en/2023/09/14/internet-oppressors-a-look-at-the-office-of-irans-attorney-general-and-its-contractors/.

64 "Internet Oppressors: A Look at the Office of Iran's Attorney General and its Contractors," Filterwatch, September 14, 2023, https://filter.watch/en/2023/09/14/internet-oppressors-a-look-at-the-office-of-irans-attorney-general-and-its-contractors/.

65 "German-made cameras used to catch Iranian women defying hijab ban," Jörg Luyken, The Telegraph, August 7, 2023, https://www.telegraph.co.uk/world-news/2023/08/07/bosch-sold-cctv-cameras-iran-identify-women-without-hijabs/.

In its current state, Nazer is a suite of software that covers various aspects of public and private life and relies on the participation of "spontaneous public forces" or vetted volunteers who act as hijab enforcers and use the Nazer app to report offenders. This policy effectively gives moral policing powers to private citizens.

In all, Nazer is a digital tool for repression and surveillance and lets police officers or volunteers make decisions without substantive judicial oversight.

LIFESTYLE MONITORING SYSTEM

The proposed "Lifestyle Monitoring System," outlined in the Seventh Development Plan Bill, is a far-reaching and evasive data collection initiative intended to enhance the profiling capabilities of government agencies.[66] This initiative, a collaborative effort between the Ministry of Culture and Islamic Guidance and the Statistical Center of Iran, seeks to gather a wide set of data on various dimensions of the lives of individuals, including living conditions, health, transportation, judicial status, and administrative activities. The system's stated goal is to "facilitate citizens' lives," suggesting an aim to streamline and possibly personalize government services. Under the proposed legislation, government bodies, public service providers, and private companies, including online taxi operators, e-commerce platforms, and other digital services handling Iranian user data, must continuously upload this data to the "System for Monitoring, Evaluating, and Continuously Measuring Public Culture and Lifestyle Indicators," also known as the Lifestyle Monitoring System. This extensive data collection is enabled by the architecture of the NIN, which includes both pre-existing infrastructure and service layers. The government's policy of forcing Iranian users to migrate to domestic applications and services further strengthens these data sources.

However, this central data collection, without adequate legal data protection and given the Islamic Republic's human rights track record, poses significant risks to the personal security and privacy of Iranians. The Lifestyle Monitoring System would permit law enforcement and judicial agencies to access personal data without adhering to legal procedures that guarantee data privacy and related rights. Additionally, there is growing concern among experts that the system's database could be exploited, using artificial intelligence, to profile citizens.[67] For example, the government could analyze various data points to infer individuals' political orientations, potentially classifying them as opponents of the state. Such algorithms could also likely predict the future behaviors of these individuals. Furthermore, the potential implementation of a social credit system by authoritarian regimes poses a significant risk, where individuals with low scores could progressively be denied access to public services through AI-based automatic decision-making.

HIJAB AND THE WAR ON CONTENT CREATORS

Iranian authorities continue to put direct pressure on content creators in the form of threats, interrogations, arrests, and punitive measures against online activists, social and political figures, celebrities, and influencers. As an example, on October 17, 2022, security forces arrested Mozhgan Ilanloo, an Iranian filmmaker and documentary director, in Tehran after she posted photos of herself without the mandatory hijab on Instagram.[68] The Revolutionary Court sentenced her to six years in prison for assembly and collusion against national security, 15 months for propaganda against the regime, 15 months for disturbing public order, and 15 months for encouraging immoral acts. Additionally, she was sentenced to 74 lashes and a fine of 80 million Iranian Rials payable to the state treasury.[69] Ilanloo's case highlights the severe consequences activists and women who use online spaces to express dissent from the Islamic Republic's moral and political mandates face.

In response to the Women, Life, Freedom movement, the Iranian police also launched the "Warden Initiative" on April 15, 2023, which aims to stem hijab non-compliance.[70] This initiative explicitly aims to go after public figures who personally reject the compulsory hijab or promote not wearing hijab or other acts deemed indecent. By May 2023, driven by aggressive increased online surveillance, officials claimed the initiative had identified and reported over 10,000 offending individuals and reported them to the police.[71] Officials also reported the initiative led to over 300 arrests, hundreds of official warnings, summonses, content removal, and at least 1,300 websites and social media accounts being investigated or taken down.

---

66 "Iran's "People's Lifestyle Assessment System": A New Surveillance Threat," Louis Shikabi, Filterwatch, December 14, 2023, https://filter.watch/en/2023/12/14/irans-peoples-lifestyle-assessment-system-a-new-surveillance-threat/.

67 "'Monitoring Lifestyle' in Iran and the Nightmare of Artificial Intelligence in the Absence of Legal Guarantees," Louis Shakibi, Filterwatch, December 23, 2023, https://filter.watch/en/2023/12/14/irans-peoples-lifestyle-assessment-system-a-new-surveillance-threat/.

68 "Mojgan Ilanlou has been arrested," Donya Eqtesad, August 21, 2023, https://donya-e-eqtesad.com/%D8%A8%D8%AE%D8%B4-%D8%B3%D8%A7%DB%8C%D8%AA-%D8%AE%D9%88%D8%A7%D9%86-62/3995154-%D9%85%DA%98%DA%AF%D8%A7%D9%86-%D8%A7%DB%8C%D9%84%D8%A7%D9%86%D9%84%D9%88-%D8%A8%D8%A7%D8%B2%D8%AF%D8%A7%D8%B4%D8%AA-%D8%B4%D8%AF.

69 "'Mojgan Ilanlou' sentenced to 10 years in prison and 74 lashes," Shargh Daily, January 17, 2023, https://www.sharghdaily.com/%D8%A8%D8%AE%D8%B4-%D8%B3%DB%8C%D8%A7%D8%B3%D8%AA-6/867499-%D9%85%DA%98%DA%AF%D8%A7%D9%86-%D8%A7%DB%8C%D9%84%D8%A7%D9%86%D9%84%D9%88-%D8%A8%D9%87-%D8%B3%D8%A7%D9%84-%D8%B2%D9%86%D8%AF%D8%A7%D9%86-%D8%B6%D8%B1%D8%A8%D9%87-%D8%B4%D9%84%D8%A7%D9%82-%D9%85%D8%AD%DA%A9%D9%88%D9%85-%D8%B4%D8%AF.

70 "Hijab Legislation in Cyberspace: the Government Expands its Efforts to Suppress Personal Freedoms in Iran," Pooyesh Azizeddin, Filterwatch, September 24, 2023, https://filter.watch/en/2023/09/24/fatawatch-april-july-2023/.

71 "Police Spokesperson: 301 people arrested in the implementation of the chastity and hijab plan," June 14, 2023, https://www.asriran.com/fa/news/894014/.

To provide stronger legal backing to policies like the Warden Initiative, the ultra-conservative Iranian government and parliament collaborated in developing the "Bill to Support the Culture of Chastity and Hijab."[72] The bill enumerates new criminal offenses and harsh penalties for non-adherence to compulsory hijab and proper attire, nudity, and indecency and creates a set of enforcement duties for various state agencies. The bill was drafted by the Iranian judicial and executive branches in the spring of 2023. The Parliament passed the bill twice in September and October of 2023, but in both instances, it was rejected by the Iranian Guardian Council, which must veto laws if they are not deemed compatible with Islamic law and Iran's Constitution. The bill was revised and passed, and on March 8, 2024, which was International Women's Day, it was resubmitted to the Guardian Council. As of this writing, the bill is still pending Guardian Council approval.

A key aspect of the Hijab Bill is that it explicitly covers activities in cyberspace and does so regardless of the platforms or their country of origin. This bill even suggests harsher penalties for violating hijab standards in cyberspace than in physical public spaces. If the bill is approved, the new criminal penalties will come into place just as the Islamic Republic looks to increase its online surveillance capacities significantly.

Under the March 2024 version of the bill, promoting nudity, indecency, lack of hijab, or inappropriate attire through social media is punishable by imprisonment and a fine (Article 38). Similarly, insulting the hijab or promoting nudity or indecency online or through social and online networks can incur fines, travel bans, restrictions on internet activity, and content removal (Articles 39 and 41). In addition to these penalties, celebrities found guilty of promoting nudity or improper attire can also be punished with the seizure of their assets or termination from their job.

Concurrently with efforts to potentially criminalize content deemed objectionable, the proposed Seventh Development Plan of November 2023 outlines a directive for the Islamic Republic of Iran Broadcasting Service and the Ministry of Culture and Islamic Guidance.[73] Their mandate under this plan is to generate content that embodies "Iranian-Islamic culture" and to combat "psychological and cultural aggression." The objective is to establish state-sanctioned content as a substitute for that which is not approved. This strategy aligns with the NIN framework, aiming to encourage the transition to domestic platforms and reduce reliance on international ones.

---

72 "Hijab Legislation in Cyberspace: the Government Expands its Efforts to Suppress Personal Freedoms in Iran," Filterwatch, September 24, 2023, https://filter.watch/en/2023/09/24/fatawatch-april-july-2023/.

73 "How the Iranian Parliament Plans to Spy on Citizens with the 'Lifestyle Assessment System,'" Louis Shakabi, Filterwatch, October 30, 2023, https://filter.watch/en/2023/10/30/policy-monitor-oct-2023/.

5

THE IMPACT OF SANCTIONS ON INTERNET ACCESS

In recent years, U.S. foreign policy has significantly influenced Iran's relationship with the global internet. While various sanctions have been imposed on Iran since the 1979 Iranian Revolution, the most specific and stringent restrictions were prominently reinstated and expanded starting in 2018. Broad U.S. sanctions have long prohibited any U.S. company from conducting business with Iran. Since 2018, these restrictions also apply to non-U.S. companies whose activities involve the U.S. in any direct or indirect manner, including transactions processed through U.S. banks or payment systems.[74]

One result of these extraterritorial sanctions is that many Iranian companies, websites, and users have been kicked off international servers and services, including those based in Europe.[75] This development accelerated the process of internet localization by forcing Iranians and Iranian businesses to migrate onto the NIN's infrastructure, cloud storage, and services, which are fully exposed to government surveillance, private data collection, and information controls.

In 2019, a tech activist created and maintained a list on GitHub of 282 companies that had blocked their services to Iran-based IP addresses. Even free services, such as free Adobe products, have been unavailable to Iranian users. Iranian developers, unable to utilize international cloud-hosting services and development tools, face challenges creating their own anti-surveillance and anti-censorship applications to bypass government-imposed internet restrictions and increase the security of under-data. Leading providers, including Google Cloud, Amazon Web Services (AWS), DigitalOcean, and GoDaddy, continue to withhold their offerings from the Iranian market, thereby impeding the nation's ability to engage in secure and efficient digital exchanges. In some cases, these international tech firms are risk-averse and over-comply with sanctions.

Consequently, Iranians are still largely cut off from a wide range of international communication tools and services, adversely affecting information access and digital security across society. This highlights the impact of existing economic sanctions, promoted by them or their partners, on the ability of Iranians to access online tools and services.

The U.S. Treasury's Office of Foreign Assets Control (OFAC) introduced General License D-1 in February 2014 and General License D-2 in September 2022, clarifying that tech firms can provide or sell personal and commercial communication tools and services to Iranians, including messaging apps, VPNs, satellite internet hardware, e-gaming, e-learning platforms, automated translation, and user authentication services.[76] These broad authorizations allow all U.S. persons and entities to engage in specified activities without applying for a separate license.

Nonetheless, these general licenses have done little to persuade tech firms that they can provide their communications services to Iranians. While OFAC remained open to evaluating requests for specific licenses, companies have had little economic incentive to invest in the complex application process and compliance requirements of specific OFAC licenses.

The effectiveness of specific licensing policies greatly depends on the response of the management of relevant sites and companies. Additionally, sanctions have cut Iranians off from the international banking system and international financial services, making it extremely difficult to purchase international online services, such as VPNs or satellite internet, regardless of their legality.[77]

To date, the open-source code library GitHub has been the only major tech enterprise to embark on a lengthy application and invest in a parallel advocacy process to gain a specific license from OFAC. For two years, GitHub argued its

---

74 "Iran Sanctions," OFAC, US Department of Treasury, https://ofac.treasury.gov/sanctions-programs-and-country-information/iran-sanctions.

75 "Locked out: Why is Amazon blocking Iranians from its services?" Maziar Motamedi, Al Jazeera English, October 2, 2019, https://www.aljazeera.com/economy/2019/10/2/locked-out-why-is-amazon-blocking-iranians-from-its-services.

76 "U.S. Treasury Issues Iran General License D-2 to Increase Support for Internet Freedom," US Department of Treasury, September 23, 2022, https://home.treasury.gov/news/press-releases/jy0974.

77 "'Maximum Pressure' US Economic Sanctions Harm Iranians' Right to Health," Human Rights Watch, October 29, 2019, https://www.hrw.org/report/2019/10/29/maximum-pressure/us-economic-sanctions-harm-iranians-right-health.

services promoted free speech and the free flow of information. Finally, in January 2021, GitHub announced that it had secured a U.S. government license to offer its services to developers in Iran.[78]

The European Union has limited its sanctions to individuals and entities allegedly deemed to have been involved in serious human rights violations, including internet censorship and surveillance.[79] These sanctions have sent a strong message to the Islamic Republic and, in theory, created a basis for some accountability for abusers. In some instances, however, EU sanctions have inadvertently but notably harmed Iranians' internet access.

Overall, poorly constructed sanctions have effectively bolstered Iranian state policies by accelerating localization, limiting access to international services, and hurting access to safe VPNs. These policies, some aimed at supporting internet users, undermine the broader goal of promoting freedom of expression, access to information, and privacy in restrictive environments.

---

78 "Advancing developer freedom: GitHub is fully available in Iran," Nat Friedman, Github, January 5, 2021, https://github.blog/2021-01-05-advancing-developer-freedom-github-is-fully-available-in-iran/.

79 "EU sanctions against Iran," Council of the European Union, https://www.consilium.europa.eu/en/policies/sanctions-against-iran/.

6

POLICY RECOMMENDATIONS

This report offers the following actionable recommendations to European governments that would enhance internet freedom in Iran. The goal is to mitigate censorship, ensure access to information, and hold the Iranian government accountable for internet disruptions. These recommendations aim to empower Iranians to exercise their fundamental human rights through a free and secure internet.

1. INVEST IN VPNS, CIRCUMVENTION & ALTERNATIVE TECHNOLOGIES FOR INTERNET ACCESS

a. Urgently allocate funding to VPNs and circumvention technologies.

i. As explained throughout this report, the Iranian population heavily relies on VPNs and circumvention tools to bypass censorship, access information, and communicate safely. However, there continues to be a shortfall in funding for free and secure VPNs for Iranians. Germany and the EU should allocate funding to support the development, maintenance, and distribution of VPNs and circumvention technologies. These tools are essential for Iranians to exercise their fundamental human rights online.

b. Prioritize "next generation" and "cutting-edge" technologies.

i. As Iran's censorship systems become more complex, there is a strong need for innovation in bringing about more censorship and shutting down resistant circumvention and security tools. Europeans should allocate funding specifically to supporting new and more advanced forms of VPNs and other internet freedom technologies.

2. INVEST IN PROGRAMMING FOR DIGITAL SECURITY

a. Promote digital security practices in Iran.

i. As explained throughout this report, Iranians, including activists and journalists, face significant risks due to surveillance and censorship. Actionable steps that Europeans can take to promote safe digital practices in Iran include:

1. Developing engaging public campaigns that raise awareness about digital security practices;

2. Providing accessible resources in Persian, including guidelines on secure communication, privacy, and anonymity;

3. And supporting help desks to respond to urgent security needs and provide real-time assistance.

3. HOLD THE IRANIAN GOVERNMENT ACCOUNTABLE

a. European states should act at the International Telecommunications Union (ITU), including drafting a submission to the ITU, to ensure Iran is transparent and held accountable to the body's rules. European states should advocate for the following policies at the ITU.

i. Iran's information control policies offend the ITU's goals, including efforts to attain "meaningful connectivity" and achieve the Sustainable Development Goals.[80] The ITU's approach thus far has overlooked the broader implications of Iran's restrictive Internet policies, which violate the rights of millions of Iranians to access information and communicate freely.

ii. The ITU should hold Iran accountable for its censorship and surveillance. If Iran violates ITU rules or disrupts Internet connectivity without proper notification and justifiable reasons, the ITU should impose appropriate penalties.

iii. The ITU should call on Iran to stop internet shutdowns, as it has rightfully done in other countries'

80 "Aspirational targets for 2030," ITU, https://www.itu.int/itu-d/meetings/statistics/umc2030/.

contexts, and consider their negative impact on communities.[90]

iv. The ITU should insist that Iran promptly notifies it about any internet shutdowns or disruptions. Iran should be obliged to provide a comprehensive and transparent account of the actions that have led to such shutdowns, as mandated under the ITU Constitution. This transparency is essential for the ITU's ability to monitor and respond effectively to these issues.

v. The ITU's annual report rankings should also include a review of the effects of internet shutdowns in countries like Iran.

vi. The ITU should support the rights of Iranians to access uncensored and secure satellite internet.

4. IMPLEMENT TARGETED SANCTIONS WITH VIGOROUS HARM ASSESSMENTS

a. The European Union should sanction Iranian officials, individuals, and entities directly involved in digital censorship and surveillance.

i. Priority should be given to identifying and sanctioning high-ranking officials directly responsible for internet shutdowns.

ii. Any sanctions considered should first undergo comprehensive harm assessments before imposition to ensure minimal harm to the general populace. Such harm assessments should include broad consultation with experts.

b. Avoid targeting infrastructure-level technologies.

i. Critical infrastructure-level technologies (e.g., internet gateways, service providers, data centers) are fundamental for internet access. Sanctioning entities that deliver technologies and services poses a high risk of inadvertently limiting Iranians' access to a free and secure internet. Germany and the EU should adopt clear policies that avoid sanctioning entities involved in infrastructure-level technologies.

5. SANCTION INTERNATIONAL COMPANIES SUPPLYING SURVEILLANCE AND CENSORSHIP APPARATUS

a. Subject international companies to sanctions.

i. International companies are supplying facial recognition technology and other censorship and surveillance tools and services to Iran's security apparatus. These companies should be investigated, and sanctions should be enforced by identifying relevant entities operating within European jurisdictions.

6. ENCOURAGE EUROPEAN BASED CLOUD PROVIDERS AND TECH FIRMS TO ENABLE SECURE SERVICES FOR IRANIANS

a. European-based cloud providers should:

i. Support access to their infrastructures and explore alternative payment channels (e.g., cryptocurrency) for Iranians. European cloud providers should also enable Iranians to set up their own VPNs using international infrastructures.

ii. European cloud providers should partner with international VPN providers that are dedicated to providing free services to Iranians. Cloud providers should help these VPNs set up cost-effective and resilient networks.

b. European-based tech firms should:

i. Integrate circumvention into communication tools (e.g., Wire, Pleroma) and offer them free of charge to Iranian users. They should also develop guidelines for seamless integration, emphasizing strong encryption and minimal performance impact.

---

81 "Netanyahu warns of a long and difficult fight," NBC News, October 29, 2023, https://www.nbcnews.com/news/world/live-blog/israel-hamas-war-live-airstrikes-gaza-ground-operation-rcna122596.

ABOUT THE AUTHOR

The Miaan Group is a nonprofit organization founded in 2019 to promote human rights, good governance, and social justice in Iran and the broader Middle East. Our team of experienced journalists, human rights lawyers, security experts, and researchers provides legal, technical, and advocacy support to human rights organizations and defenders in Iran. Since 2022, Miaan has run Filterwatch, a research hub for Iranian internet policies, and Iran After Dark, an online resource center for internet shutdown preparedness.

IMAGE RIGHTS AND COPYRIGHT INFORMATION

Image 1: Screenshot of Jam e Jam Newspaper Cover
Date of Publication: November 20, 2019; Location: Tehran
The screenshot of the cover of Jam e Jam newspaper, published on November 20, 2019, in Tehran, is used here for informational purposes. All rights to the original content belong to Jam e Jam newspaper. The image is reproduced under fair use guidelines for the purpose of commentary, criticism, news reporting, or educational use. For any other use, permission must be obtained from the copyright holder, Jam e Jam newspaper.

Image 2: Screenshot Nazer App
The screenshot from the Nazer App provided here has been supplied by a confidential source who wishes to remain anonymous. All rights to the original content of the app are owned by the app's developer or publisher. This image is reproduced under fair use guidelines for the purpose of commentary, criticism, news reporting, or educational use. For any other use, permission must be obtained from the copyright holder, which is the app'sdeveloper or publisher.

IMPRINT

Published by:
Friedrich-Ebert-Stiftung e. V.
Godesberger Allee 149
53175 Bonn
Germany
Email: **info@fes.de**

Issuing Department:
Friedrich-Ebert-Stiftung | Department for Middle East and North Africa | Hiroshimastr. 28 | 10785 Berlin | Germany

Responsibility for content and editing:
Marcus Schneider | Director | Project on Peace and Security in the MENA Region

Contact/Order: **info.nahost@fes.de**

Design: pertext | www.pertext.de

ISBN 978-3-98628-492-3

THE INTERNET IN THE WOMEN, LIFE, FREEDOM ERA

Iran's Progress in Censorship and Surveillance – and Options for European Policymakers

This report discusses Iran's National Information Network (NIN), a system designed to control and surveil internet usage. The NIN was intensified in response to the »Women, Life, Freedom« movement, which marked a significant shift in Iran's socio-political landscape. The NIN is an internet localization project aimed at isolating Iranian users from the global internet, giving the Islamic Republic maximum control over content, connectivity, and private user data.

The Iranian government has responded to the »Women, Life, Freedom« movement with an aggressive crackdown extending to online spaces. Policymakers are developing a more sophisticated surveillance framework to consolidate control over the population, maintain social order, and enforce religious and ideological mandates. This includes the development of domestic internet platforms and services and using other technologies for reporting hijab violations, such as facial recognition systems.

This report concludes with policy recommendations addressed to the European Union and Germany for improving internet access and freedom in Iran, addressing the needs and concerns of various stakeholders. These include investing in VPNs, circumvention, alternative internet access technologies, digital security programming, holding the Iranian government accountable, implementing targeted sanctions with vigorous harm assessments, and encouraging European-based cloud providers and tech firms to enable secure services for Iranians.

Further information on the topic can be found here:
https://www.fes.de/referat-naher-mittlerer-osten-und-nordafrika

FRIEDRICH EBERT STIFTUNG