During Iran's nationwide internet shutdowns in 2025–2026, the extended blackouts sharply limited access to global communications and information and reflected the Islamic Republic's growing ability to control digital connectivity through the National Information Network (NIN), a system discussed throughout this paper. Shutterstock Asset ID 2724085803

From Coercion to Code: Iran's Digital Security Transformation

Paola Maria Raunio and John Hatzadony

Introduction

Prior to the start of the protests in Iran on December 28, 2025, social media platform X began displaying the approximate user locations of certain Iranian accounts. Close inspection revealed an unexpected pattern: Most Iranian citizens had experienced some internet restrictions during previous rounds of civil unrest. However, some individuals, including figures who publicly claimed to be under persecution, managed to maintain stable connectivity. Media investigation suggests that these users, who possessed special credentials granting them unfiltered internet access during the nationwide shutdown, were able to promote narratives aligned with official positions while independent voices remained offline.[1]

Two months later, we witnessed how selective connectivity was deployed under circumstances that had created an existential crisis for Iran. When the United States and Israel launched military strikes against Iran on February 28, 2026, authorities continued the near total internet blackout that had hardly been lifted since the most recent round of protests, reducing connectivity to the outside world to just 1 percent of ordinary levels.[2] Yet Iranian officials continued to appear on international media. Foreign Minister Abbas Araghchi conducted a live interview with CBS via Zoom, even as millions of Iranians were cut off from information that could have helped them navigate the military attacks. What had been used as a tool of narrative control during domestic protests became, under wartime conditions, an instrument of political control.

Iran's response to internal security threats has been undergoing rapid digital transformation. From the Green Movement unrest of 2009 to recent nationwide protests at the end of December 2025, Iran has evolved its approach away from reactive, kinetic power to a continuous, multitiered system of digital repression.[3] This paper documents this shift across three periods: 1) the 2009 protests, which revealed systemic shortfalls; 2) the following ten years of network consolidation and technical development, along with reliance on homegrown platforms; and 3) the period after 2002, marked by the application of facial recognition, pattern-tracking, and digital enforcement tools. The paper also touches on the unprecedented stress test that the 2026 war imposed on the entire apparatus. At the time of writing, it is factually hard to assess and verify how the country's digital control and monitoring infrastructure has been impacted by the war. But, at the same time, we have witnessed how the authorities have stayed in power

and continued to control digital infrastructure, at least in terms of wartime information management.

The analysis that follows documents this transformation. Through available evidence, it traces the institutional investments, technical capabilities, and operational deployments that constitute Iran's current digital governance architecture. The implications extend well beyond Iran's borders. This transformation carries significant implications for regional security and stability, technology governance, and the broader question of how states may leverage digital tools for social control. Policymakers assessing Iranian capabilities, technology firms evaluating engagement decisions, and analysts tracking the regional diffusion of digital control techniques all have reason to take notice.

The 2009 Protests: Catalyst for Change

The June 2009 presidential election sparked the biggest protests since 1979. Millions protested after official results unexpectedly declared incumbent Mahmoud Ahmadinejad the winner by a wide margin, despite exit polls indicating that Mir Hossein Mousavi was ahead in the polls. The government crackdown exposed both its strengths and weaknesses. Authorities mobilized foot patrols, regular militia units, and plainclothes agents to disperse protesters. Officials also banned protest permits. Security forces employed pellet rifles, batons, and tear gas to disperse protesters; authorities allegedly deployed snipers on city streets; and intelligence agencies cracked down on high-profile activists. As of late September, some four thousand protesters had been arrested.[4] The government, for its part, reported that no more than thirty-six to thirty-seven protesters had been killed during the crackdown, while human rights groups

claimed that the number of victims was closer to eighty—nearly double.[5] The internationally publicized death of Neda Agha-Soltan, a 26-year-old woman shot during a protest on June 20, 2009, focused additional attention on Iran. Witnesses captured her death on cell phone videos that quickly spread worldwide. Iran faced international criticism and was met with further sanctions in response

Authorities also attempted to restrict information flow by slowing text messages and blocking social media sites like YouTube and Facebook. These measures proved inadequate. Protest imagery and videos continued circulating through alternative channels. Protesters coordinated through platforms authorities could not control. The government won the street battle but decisively lost the information war.

Post–protest measures revealed the limitations of available tools. Traditional, labor-intensive, person-to-person surveillance methods generated resentment and achieved only temporary compliance. Authorities published photographs of unidentified protesters and offered rewards for identification. Shopkeepers, whose property had been damaged, and doctors, treating the injured, were offered governmental compensation if they agreed to file written complaints against unidentified demonstrators. The introduction of some six thousand units, which recruited teachers and pupils in primary schools, enabled the security apparatus to penetrate families and scrutinize private beliefs. However resource-intensive these methods were, the compliance they produced proved neither deep nor lasting.

Data from the Digital Society Project confirms this assessment. The government-control-over-society indicator spiked to 3.84 out of 4.00 in 2009, indicating a maximum physical control effort, before dropping to

3.11 in 2010, a pattern reflecting unsustainable resource deployment. Meanwhile, internet filtering capacity and narrative control capacity both registered only 2.00, indicating a moderate technical ability to block specific platforms but no comprehensive digital control capability.[6]

The 2009 events thus exposed three critical gaps: physical enforcement proved resource-intensive and generated international costs; information control capabilities were inadequate; and visible coercion created symbols of resistance rather than compliance. These gaps drove the subsequent investment.

Building Digital Infrastructure: 2010–2022

The decade following the 2009 protests saw the systematic construction of digital governance capabilities across institutional, technical, and operational domains.

Institutional Coordination

New coordinating bodies centralized digital policy. The Supreme Council for Cyberspace, established in 2012 under the Supreme Leader's oversight, coordinates policy across agencies; the National Cyberspace Center operationalizes its decisions; and the Cyber Police Force (FATA), created in 2011, monitors online activity, with an explicit mandate to protect national and religious values in digital spaces.[7] These bodies complement existing intelligence structures, creating a permanent bureaucratic capacity for digital governance that did not exist in 2009.[8]

Network Infrastructure

The centerpiece of Iran's digital infrastructure is the National Information Network (NIN), development of which began around 2010. NIN creates a managed domestic internet ecosystem that enables graduated control responses unavailable in

2009. Its architecture permits authorities to restrict specific platforms, throttle data transfer rates to specific regions, and implement localized shutdowns targeting protest hotspots while preserving access to approved domestic services.[9]

NIN's design minimizes the costs of internet restrictions. During disruptions, citizens retain access to banking, government services, and approved domestic applications. This selectivity reduces both economic damage and civilian frustration compared with complete disconnection, lowering the political cost of network control. That said, authorities still find it difficult to avoid political and economic costs altogether. During the December 2025–January 2026 economic protests, weeks-long shutdowns generated significant frustration as e-commerce businesses experienced extensive losses.[10] NIN's architecture represents a substantial advance over the crude blocking of 2009, but it has not eliminated the costs of digital coercion.

Forced Localization

International sanctions accelerated the development of domestic alternatives to foreign services. Applications such as Rubika, Eitaa, and Soroush, developed by government-connected entities, became mandatory for accessing e-government services, educational platforms, and banking. These platforms serve a dual purpose: essential functionality for users and surveillance and data collection capabilities for the state that would be unavailable through foreign services.[11]

During the 2022 protests, these platforms became key data collection vectors precisely because protesters, like all Iranians, had no choice but to continue using them for essential services. This forced dependence created comprehensive monitoring that foreign platforms could

never provide. The mandatory nature of domestic platforms transformed ordinary app usage into inescapable surveillance.

Technology Transfer

Bilateral agreements expanded Iran's technical capabilities. Through bilateral deals, including a twenty-five-year deal signed in 2021 with China, Iran has acquired access to monitoring technology, such as facial recognition cameras.[12] Iranian officials have framed these collaborations as assertions of digital sovereignty.

Narrative Control Infrastructure

In 2019, Iran established the Baqiatallah headquarters to centrally coordinate and manage pro-government soft war and cultural initiatives across Islamic Revolutionary Guard Corps (IRGC) and Basij entities.[13] This institutional structure represents a deliberate shift from 2009's ad hoc censorship toward professional, centrally coordinated information operations.

Beginning with the 2022 protests, the Seraj organization, operating under Baqiatallah, conducted systematic messaging campaigns. These included spreading disinformation, exaggerating security force presence, inflating protester casualty numbers, promoting conspiracy theories around the death of Mahsa Amini, and manipulating social media hashtags by trending deliberately misspelled versions of #MahsaAmini to disrupt global awareness.[14] The coordinated nature of these campaigns demonstrates a qualitative advancement in narrative control.

Prototyping and Iteration

The wave of economic protests in 2017–2018 allowed for some prototyping of future capabilities. Officials experimented with localized internet shutdowns affecting select provinces while leaving the rest of the

country online—a tool Iran did not possess in 2009. These protests also saw the first instances of social media surveillance resulting in pinpoint arrests instead of wholesale ones. Lessons from these protests were taken on board.

Further development of the necessary infrastructure was justified and accelerated by the COVID-19 pandemic. Enforcement of Covid protocols allowed authorities to mandate downloads of tracing apps, like A-19 and Mask.ir, that required personal information and location tracking permissions from users.[15] The pandemic accelerated plans for government services to go digital, ranging from telehealth to web-based university registrations, all of which needed application downloads that enabled surveillance. By categorizing expanding surveillance as a public health requirement, the Covid pandemic gave the regime license to expand its surveillance infrastructure in ways that could be exploited during the 2022 uprisings. By 2022, Iran had a centralized oversight apparatus, a full suite of network disruption tools, with much of the population on domestic platforms, allowing user data profiling and surveillance technology for mass identification of users.

The 2022 Protests: New Digital Capabilities on Display

Few situations since 1979 have threatened the authorities like the nationwide protests that erupted after the death of Mahsa Amini in September 2022. Nearly every capability honed over the past decade was leveraged during this period of civic unrest. Protests took place in every province and represented cross-sectional participation from every ethnic, regional, and class constituency. Participation by women was widespread, with the removal of headscarves in public serving as a symbol of the protests. There have been more than 22,000 detentions, 7,000 injured, and 551 killed, according to the United Nations.[16]

Iranian authorities attributed the violence to foreign-backed elements; human rights organizations attributed the casualties primarily to security forces.

Internet access was restricted for approximately two weeks during peak protest activity. Instagram, the last major international platform accessible in the country and a primary channel for documenting demonstrations, was blocked.[17] Unlike the ad hoc measures of 2009, NIN architecture enabled authorities to maintain domestic services while restricting international access. The Digital Society Project's internet filtering-capacity score rose from 2.00 in 2009 to 4.00 in 2022, indicating maximum technical capability. Shutdown capacity similarly reached 4.00, confirming the transformation in network control.[18]

Active information operations did not stop at blocking alone. Pro-regime accounts pushed alternative narratives, denied death tolls, and accused foreigners of manipulation. Doxed protestors received barrages of personalized attacks, coordinated across pro-regime accounts that sought to shame them into silence. Ali Karimi—a celebrated Iranian footballer, with more than 15 million followers on social media, who had voiced support for the protests—was relentlessly mocked by pro-government accounts for purportedly protesting so that he could obtain asylum abroad. Actresses who expressed support for the protests were arrested and sentenced to government-run psychiatric sessions once a week for being mentally ill. Photos of these actresses receiving "treatment" were then circulated across pro-regime accounts. This tactic showed how capable authorities were of weaponizing not just arrests but the information campaign against doxed individuals.[19]

White SIM Cards: Infiltrating Opposition Discourse

Accounts that continued to tweet during internet blackouts, after obtaining access through official channels, pushed pro-regime talking points while independent voices were silenced. Access credentials were given to individuals who had already publicly cast themselves as members of the opposition; some had even alleged prior victimization through arrest or imprisonment at the hands of the regime. However, these accounts were activated during internet blackouts to harass legitimate activists, promote divisive language, and muddy the conversation about whether an opposition movement truly existed.[20]

The regime placed outspoken critics at the helm of managing the opposition conversation to internally divide dissent while obscuring its hands in the manipulation of information. Iran's state-narrative-dominance score was raised from 2.00 in 2009 to 3.50 in 2022 due to shrinking opportunities for dissenting voices to reach domestic audiences.[21] This same tactic of network manipulation was exercised during the Israeli bombings of Iran's nuclear program in June 2026. Whether the threat is domestic unrest or foreign invasion, NIN has proven itself as a mobilized arsenal to suppress whatever the regime deems threatening at any given moment. Memes featuring AI-generated images of Iranian soldiers defeating Israeli forces flooded domestic media channels during the conflict.[22]

Post-2022: Automated Surveillance and Compliance

Authorities have continued to expand their digital infrastructure since 2022 for comprehensive surveillance and automatic flagging. Already under development in 2019–2020, with the help of outside developers, facial recognition systems are installed on transit hubs, roads, and

university campuses nationwide and cross-referenced with ID photos stored in Iran's official databases.[23] In spring 2025, regulations extended camera requirements to residential and commercial buildings with four or more units, with feeds accessible to law enforcement through centralized cloud servers.[24] Drones equipped with AI-powered recognition software have since been deployed to monitor public spaces, particularly to enforce modesty laws.[25]

In 2023, Nazer, an official government application that allows civilians to report violations of clothing regulations by inputting a car's license plate or an individual's social media handles, was released. Citizens who are identified as being dressed improperly receive automated warnings from the government.[26] This not only outsources surveillance to the general public; it also exponentially increases surveillance capacity.

The government also announced the creation of the Lifestyle Assessment System in 2023. Ostensibly, this system will analyze a citizen's behavior in several categories. Allegedly scanning through an individual's internet history, social media activity, GPS location data, purchasing history, and interactions with government agencies, the system will cross-reference this information with live surveillance to assess each individual's behavior in real time.[27] Citizens do not appear to have been assigned scores yet. But if individuals are flagged for violating rules, they will receive automated warnings, and if they continue to reoffend, they will be unable to access government services, banks, and public transportation. In spring 2025, it was announced that citizens not adhering to dress codes would not be able to access bank accounts, government agencies, or domestic flights.[28] These non-physical punishments represent a shift from punishment requiring human enforcement

and instead coerce individuals by limiting their ability to complete everyday tasks.

Targeted surveillance complements mass monitoring. The SIAM system, enabled by the state's acquisition of major telecommunications companies in 2009, permits message decryption, location tracking, and metadata analysis.[29] Individuals posting content deemed problematic report experiencing data throttling when attempting uploads, with restrictions lifting only after receiving official warnings.[30] This uncertainty about what triggers monitoring potentially induces broader self-censorship across the population.

International Mobile Subscriber Identity (IMSI) catchers enable localized identification of mobile devices. Reports indicate morality police monitor CCTV footage. When violations are observed, field agents equipped with IMSI catchers are dispatched to identify the person. The state has also developed malware to carry out targeted data collection. VPNs from other countries have been banned by the state; however, VPNs from Iran have been sold as parental controls or employee monitoring software. Security analysts found that malware named EyeSpy was built into Iranian VPN software to record passwords, documents, images, and keystrokes. [31] Authorities have been secretly weaponizing citizens' go-to circumvention tools.

The 2026 War: Stress Test

On February 28, 2026, the United States and Israel launched a coordinated military campaign against Iran. The first round of strikes targeted Iran's military installations and government facilities, killing Supreme Leader Ali Khamenei and other senior officials. Iran's retaliatory missile and drone attacks have targeted Israel and U.S. bases and assets across the Middle East. The conflict, which has entered week six and a fragile two-week ceasefire at

the time of writing, has subjected the digital surveillance and control apparatus discussed in this paper to an unprecedented stress test. Due to the ongoing conflict and restricted access to Iran, it is challenging to verify how the tools described above have been deployed under wartime conditions. Almost no anti-government protests have been reported since the start of the war; however, more than a thousand people have reportedly been arrested since the war began. [32] What has been evident, however, is the longest network shutdown in the history of the internet and a strategic change in the operation of NIN.

The internet shutdowns discussed earlier in this paper—selective, temporary, and increasingly effective since 2009—have now taken on a qualitatively different nature. On January 8, 2026, authorities imposed a total internet blackout as a response to the protests that had started in December 2025. This blackout severed the entire nation's global internet access, limited access even to NIN and domestic online services, phone and text messaging services, and Starlink.[33] The government created almost a total digital isolation—an unprecedented act that continued almost fully enforced until the start of the current war. Following the military campaign that started on February 28, 2026, internet connectivity dropped to approximately 4 percent of normal levels.[34] Combined with the earlier shutdown caused by the protests in December–January, at the time of writing Iranian civilians have spent almost one-third of 2026 in digital isolation.[35]

The post–January and wartime shutdowns appear not to be a crisis response but a change in the authorities' digital infrastructure strategy. As reported by FilterWatch, there have been plans to cut off Iranians from the global internet and transform the country's internet infrastructure into a "Barracks Internet." [36]

In the past, NIN has been a tool to censor inappropriate content for Iranian users and block oppositional communications on foreign platforms that are harder to monitor by the authorities. But now, in this transformation, the previously restricted access would not return to ordinary citizens, and only people with security clearance on the so-called white list would have access to the global network. [37] This could be seen as the logical endpoint of the NIN strategy described in the above sections: The domestic network is not a parallel domestic network running alongside the global internet, activated at times of crisis, but a replacement for it.

The privileged white SIM card system described above has evolved during the war into an openly acknowledged tool in the authorities' digital toolbox. Ten days into the war, on March 10, 2026, Iran's government spokesperson Fatameh Mohajerani made a statement, acknowledging that "for those who can carry our voice further, opportunities will be provided." [38] The earlier-mentioned CBS interview with Abbas Araghchi on March 15, 2026, amplified this message when he was asked why he had internet access to appear in an interview via Zoom while his people remained offline; he responded, "I'm the voice—because I'm the voice of Iranians, and I have to defend their right." [39]

While at the moment it is hard to assess how the war has impacted the operation of other aspects of Iran's digital monitoring infrastructure discussed in this paper, it has pushed the authorities to re-evaluate the use of NIN and has perhaps created a strategic change in the government's approach to NIN, including permanently blocking Iranians' access to the global internet. [40]

Policy Implications

Iran's suite of digital surveillance tools has consequences that will reach beyond Iran itself. Network-level controls, mandated platforms, monitoring software, and automatic enforcement capabilities provide an example that could proliferate to Iran's neighbors via shared technology or commercial ties. It is therefore useful to first understand Iran's toolkit before considering how to react.

Iran has been pushed toward developing domestic censoring tools and sourcing technology from non-Western countries in part by Western sanctions regimes. Sanctions have not slowed Iran's capabilities in every area: During times of international technological isolation, Iran has doubled down on developing homegrown capabilities. One example is Iran's domestic AI platform, announced in March 2025 with a stable release expected "in the coming weeks."[41] Policymakers should consider if sanctions appropriately address this reality. Technology export controls are often aimed at preventing the provision of dual-use capabilities. Iran may very well be using these domestically sanctioned technologies for rights-violating purposes. The capabilities documented in this paper make dissent more expensive, more siloed, and easier to find. VPNs are unreliable, and domestic alternatives have been found to install malware on users' devices.[42] Starlink and other satellite internet services are being jammed by the regime.[43] Anyone looking to provide technical assistance to Iranians should keep this in mind. Providing a list of VPN URLs to activists does not appropriately confront the capabilities that the Iranian government maintains.

There are multiple policy avenues that should be explored. First, transfers of dual-use surveillance technology, especially facial recognition and AI software, to Iran should be monitored more closely, including

through targeted sanctions on entities selling to Iran. Second, investment should be made toward the developing circumvention tools that can function in an environment with NIN-level network controls rather than advocating that Iranians rely on commercial VPNs that go directly to a blocklist. Third, companies looking to license out dual-use technology should make efforts to understand how their technology is being used. Fourth, policymakers and those looking to assist Iranian civil society should invest in tracking developments within Iran's digital repression toolbox.

Those trying to understand the future of instability within Iran should keep in mind that the state's internal security capacity is not what it was in 2009. The Iranian government, which could not fully control the flow of information during the Green Movement, now has expansive network-control capabilities, mass surveillance tools, and automatic content enforcers at its disposal. Of course, stability is not guaranteed. Despite a powerful surveillance and punishment mechanism, Iran still saw nationwide protests in December 2025 and January 2026. If anything, the increased sophistication of Iran's control will create more backlash against the government. Instead of debating if Iran has finally been made protest-proof, we should be asking how increasing the costs of collective action changes mass mobilization. If the past few months of protest are any indication, the violence experienced by Iranians looking to speak out is only increasing.

Conclusion

The response to the 2009 protests highlighted government limitations: kinetic responses were expensive; information control was limited; and overt repression had come at a domestic and international cost. From 2009 until today, the Iranian security community has pivoted away from

kinetic responses toward building long-lasting technical foundations for information control. Throughout this period, the government has made investments across four areas: organizations like the Supreme Council for Cyberspace to govern internet management activities; Iran's National Information Network (NIN) to build capabilities for segmented infrastructure; native platforms designed for monitoring and use requirements to increase population dependence; and technology through relationships with foreign governments.

As a result, in 2022, Iran's government had three tools it did not have in 2009: the ability to exert far-reaching control over the internet to selectively deny access; censorship and propaganda capacities, which allow the government to limit not just information but also to insert and amplify its own preferred narratives; and a nascent facial recognition technology. Developments since 2022 have begun to point toward automated behavior tracking via systems such as the Lifestyle Assessment System; mandates requiring apartment complexes to install CCTV systems; user-led surveillance applications like Nazer; and propaganda across social media, television, and film meant to prime the population for future action.

Filtering gave way to "shutting down" in 2026: Iran experienced the longest nationwide internet shutdown ever. During nearly two months when internet connectivity was slashed to 1 to 4 percent of normal levels, Iranians lost access not just to the outside world but also to domestic websites, messaging apps, cellular networks, and elements of NIN. "Barracks Internet," where internet access is available in a two-tier system, keeps average Iranians in the dark for weeks while granting vetted government officials and pro-regime journalists "white list" access to social media platforms for interviews from inside

Iran—such as Foreign Minister Abbas Araghchi's interviews over Zoom during the war to spread the regime's propaganda abroad.

Iranians also paid a heavy economic price for internet blackouts, even when parts of NIN were still available. While internet blackouts lasted weeks, Iran's burgeoning e-commerce industry ground to a halt, with companies across the industry reporting that they had lost 80 to 90 percent of their revenue during shutdowns. Businesses large and small have struggled to access supplies during blackout periods, affecting every sector from pharmacies to manufacturers. The Tehran Stock Exchange fell nearly 15 percent in early 2026 as investors panicked and tried to sell off their stocks. Informal markets boomed during Iran's internet blackouts as citizens turned to cash instead of digital payments, driving the inflation rate, which hovered above 40 percent or higher. In recognition of the dire straits, the Iranian government began to offer limited and licensed internet in a rare move to revitalize parts of the economy.[44]

Limits remain: Iranians will continue to protest, they will continue to find workarounds, and the reach of Iran's tools may rebound against the government. But the capabilities built since 2009 have allowed the Islamic Republic to more heavily police the population at a lower cost than repression. For policymakers, analysts, and advocates working on Iran, knowledge of these tools, together with an understanding of their limitations, will prove important. Moreover, Iran is not alone in developing these capabilities. At issue is a shift in how a government can control a population when afforded persistent technological foundations for doing so.

Paola Maria Raunio is an assistant professor of Homeland Security at Rabdan Academy in Abu Dhabi, United Arab Emirates. She teaches intelligence and counterintelligence and her research examines authoritarian resilience, regional security in the Gulf, and the ideological dimensions of Middle Eastern politics.

John Hatzadony is the program chair of Homeland Security at Rabdan Academy in Abu Dhabi, United Arab Emirates. He specializes in intelligence and irregular warfare, with a specific focus in supply chain security and threat finance.

Endnotes

[1] Pegah Banihashemi, "Iran's White SIM Card Scandal Reveals Privilege, State Control, and Fake Dissent," *Chicago Tribune*, December 14, 2025.

[2] Netblocks (@netblocks), "Update: #Iran's Internet Blackout is Now the Longest Nation-Scale Internet Shutdown on Record in Any Country, Exceeding All Other Comparable Incidents in Severity Having Entered Its 37th Consecutive Day After 864 Hours," X (formerly Twitter), April 5, 2026, https://x.com/netblocks/status/2041057093369598241C.

[3] "Freedom on the Net 2023: Iran," Freedom House, Washington, D.C., 2023, https://freedomhouse.org/country/iran/freedom-net/2023; Iran Human Rights Documentation Center, "Violent Aftermath: The 2009 Election and Suppression of Dissent in Iran," Iran Human Rights Documentation Center, New Haven, CT, May 21, 2013, https://iranhrdc.org/violent-aftermath-the-2009-election-and-suppression-of-dissent-in-iran/.

[4] See, e.g., Simon Jeffery, "Iran Election Protests: The Dead, Jailed and Missing," *Guardia*n, July 29, 2009, https://www.theguardian.com/world/blog/2009/jul/29/iran-election-protest-dead-missing.

[5] "Iran: Election Contested, Repression Compounded," Amnesty International, London, U.K., December 10, 2009, https://www.amnesty.org/en/wp-content/uploads/2021/06/mde131232009en.pdf.

[6] Digital Society Project, "Digital Society Survey (2025)," https://digitalsocietyproject.org/data/.

[7] "Islamic Republic of Iran," Cyber Policy Portal, United Nations Institute for Disarmament Research (UNIDIR), Geneva, Switzerland, November 2023, https://cyberpolicyportal.org/states/iran-islamic-republic-of/.

[8] "Artificial Intelligence (AI) and Human Rights: Using AI as a Weapon of Repression and Its Impact on Human Rights," European Parliament, Directorate-General for External Policies Brussels, Belgium, 2024, 32, https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf.

[9] Calla O'Neill, "Iran's Digital Fortress: The Rise of the National Information Network," American Foreign Policy Council (AFPC), Washington, D.C., August 4, 2025, https://www.afpc.org/publications/policy-papers/irans-digital-fortress-the-rise-of-the-national-information-network.

[10] Michelle Nichols, "Internet Shutdown Squeezes Iran's Ailing Businesses," Associated Press, January 20, 2026, https://apnews.com/article/iran-protests-crackdown-internet-business-costs-a0bd2df1d13355dcc28f46e5b5b3c893.

[11] FilterWatch, "The Role of Domestic Messaging Apps in Iran's Information Controls," November 30, 2021, https://filter.watch/english/2021/11/30/the-role-of-domestic-messaging-apps-in-irans-information-controls/.

[12] Mariami Tkeshelashvili and Tiffany Saade, "Decrypting Iran's AI-Enhanced Operations in Cyberspace," Institute for Security + Technology, September 26, 2024, https://securityandtechnology.org/blog/decrypting-irans-ai-enhanced-operations-in-cyberspace/.

[13] Kasra Aarabi and Saeid Golkar, 'Engineering Minds and Votes: The IRGC's Baqiatallah Headquarters and Its Invisible Hand in Iran's Political Landscape,' United Against Nuclear Iran, n.d., https://www.unitedagainstnucleariran.com/sites/default/files/UANI_Engineering%20Minds%20and%20Votes.pdf.

[14] Hossein Kermani, "The Art of Delirium: Social Media Suppression in Authoritarian Regimes," *Communication Theory* 35, no. 4 (2025): 197-213, https://doi.org/10.1093/ct/qtaf006.

[15] Shahroz, Muhammad et al., "Covid-19 Digital Contact Tracing Applications and Techniques: A Review Post Initial Deployments," *Transportation Engineering*, 10, no. 5 (2021), https://doi.org/10.1016/j.treng.2021.100072.

[16] "UN: Iran Committed Crimes Against Humanity During Protest Crackdown Caused Death of Mahsa Amini," UN Watch, March 8, 2024, https://unwatch.org/un-iran-committed-crimes-against-humanity-during-protest-crackdown-caused-death-of-mahsa-amini/.

[17] Miaan Group, "The Internet in the Women, Life, Freedom Era: Iran's Progress in Censorship and Surveillance—and Options for European Policymakers," Friedrich-Ebert-Stiftung, Bonn, Germany2024, https://collections.fes.de/publikationen/ident/fes/21296.

[18] Digital Society Project, "Digital Society Survey."

[19] Shahram Akbarzadeh, Amin Naeini, Galib Bashirov and Ihsan Yilmaz, "The Web of Big Lies: State-Sponsored Disinformation in Iran," *Contemporary Politics* 31, no. 2 (2025): 337.

[20] Pegah Banihashemi, "Iran's White SIM Card Scandal Reveals Privilege, State Control, and Fake Dissent," *Chicago Tribune*, December 14, 2025.

[21] Digital Society Project, "Digital Society Survey."

[22] Matt Murphy, Olga Robinson and Shayan Sardarizadeh, "Israel-Iran Conflict Unleashes Wave of AI Disinformation," BBC, June 21, 2025, https://www.bbc.com/news/articles/c0k78715enxo.

[23] Miaan Group, "The Internet in the Women, Life, Freedom Era: Iran's Progress in Censorship and Surveillance—and Options for European Policymakers," Friedrich-Ebert-Stiftung, Bonn, Germany2024, https://collections.fes.de/publikationen/ident/fes/21296.

[24] Ata Mohamed Tabriz, "Policing Without Batons: Iran Expands Use of Tech to Preempt Dissent," Iran International, May 28, 2025, https://www.iranintl.com/en/202505285072; Mahmoud Hamidi, "Iran's Regime Introduces 'Saptam' Surveillance System for Public Monitoring," Iran News Update, October 3, 2024, https://irannewsupdate.com/news/general/irans-regime-introduces-saptam-surveillance-system-for-public-monitoring/.

[25] Mohammed Tawfeeq, "Iran is Using Drones and Apps to Catch Women Who Aren't Wearing Hijabs, Says UN Report," CNN, March 14, 2025, https://edition.cnn.com/2025/03/14/middleeast/iran-nazer-app-un-report-intl-latam.

[26] Nima Akbarpour, "'Nazer 1': A Tool for Hijab Enforcers," Medium, December 13, 2023, https://nima.medium.com/nazer-1-a-tool-for-hijab-enforcers-21bb78d5001a; Filterwatch, "Iran's

Nazer App Aims to Expand State Surveillance and Control," October 7, 2024, https://filter.watch/english/2024/10/07/irans-hijab-application-nazer-aims-to-state-expand-surveillance-and-control/.

[27] FilterWatch, "Iran's "People's Lifestyle Assessment System: A New Surveillance Threat," December 14, 2023, https://filter.watch/english/2023/12/14/irans-peoples-lifestyle-assessment-system-a-new-surveillance-threat/ .

[28] Mashregh News, "Payan-e erā'e-ye khadamāt be bi-hijāb-hā [End of Providing Services to Unveiled Women]," April 19, 2023, https://www.mashreghnews.ir/news/1481571/پایان-ارائه-خدمات-به-بی-حجاب-ها.

[29] Sam Biddle and Murtaza Hussain, "Hacked Documents: How Iran Can Track and Control Protesters' Phones," The Intercept, October 28, 2022, https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/.

[30] Miaan Group, "A Battlefield Named Isfahan: Targeted Use of IMSI-Catchers and Surveillance Cameras to Enforce Chastity and Hijab Law," April 17, 2025, https://miaan.org/a-battlefield-named-isfahan/.

[31]Claudia Glover, "Iran's Citizens Tarted by EyeSpy Spyware Hidden in VPNs," TechMonitor, January 11, 2023, https://www.techmonitor.ai/technology/cybersecurity/eyespy-spyware-iran-vpn?cf-view.

[32] Jason Burke, "Hundreds of Organized Protests Show Resilience of Iranian Regime, Experts Say," *Guardian*, March 28, 2026, https://www.theguardian.com/world/2026/mar/28/iran-pro-regime-demonstrations-detained-people.

[33] Amanda Meng, Alberto Dainotti, and Zachary Bischof, "Iran's Latest Internet Blackout Extends to Phones and Starlink," Georgia Institute of Technology, Atlanta, GA, January 16, 2026,
https://www.gatech.edu/news/2026/01/16/irans-latest-internet-blackout-extends-phones-and-starlink.

[34] NetBlocks, "Latest News," April 28, 2026, https://netblocks.org/.

[35] Cody Combs, "Internet Blackout Leaves Iranians Offline for One Third of 2026," The National, March 10, 2026, https://www.thenationalnews.com/future/technology/2026/03/10/is-iran-internet-still-down/.

[36] FilterWatch, "Iran Enters a New Age of Digital Isolation," January 15, 2026, https://filter.watch/english/2026/01/15/iran-enters-a-new-age-of-digital-isolation-2/.

[37] FilterWatch, "Iran Enters a New Age of Digital Isolation."

[38] Mahsa Alimardani, "Iran Wields Wartime Internet Access as a Political Tool," Carnegie Endowment for International Peace, Washington, D.C., March 18, 2026, https://carnegieendowment.org/research/2026/03/iran-wields-wartime-internet-access-as-a-political-tool.

[39] Abbas Araghchi, interview by Margaret Brennan, *Face the Nation with Margaret Brennan*, CBS News, March 15, 2026, https://www.cbsnews.com/news/iranian-foreign-minister-abbas-araghchi-face-the-nation-transcript-03-15-2026/.

[40] Breached Company, "Iran's 2026 Internet Blackout: 20 Days Offline, 30,000 Dead, and the Plan for Permanent Digital Isolation," February 3, 2026, https://breached.company/irans-2026-internet-blackout-20-days-offline-30-000-dead-and-the-plan-for-permanent-digital-isolation/.

[41] Silvia Boltuc, "Silicon Persia: Iran's AI Aspirations and the Global Tech Order," SpecialEurasia, March 24, 2025, https://www.specialeurasia.com/2025/03/24/iran-ai-silicon-persia/.

[42] Janos Gergo Szeles, "EyeSpy – Iranian Spyware Delivered in VPN Installers," *Bitdefender*, January 11, 2023, https://www.bitdefender.com/en-us/blog/labs/eyespy-iranian-spyware-delivered-in-vpn-installers

[43] BBC News, "Starlink Reportedly Made Free in Iran—But Protesters Are Taking Huge Risks by Using It," BBC News, January 14, 2026, https://www.bbc.com/news/articles/c0r4veg0rrzo.

[44] Lionel Prinsloo, Olga Solon, and Mark Newman, "Iran Offers Limited Internet in Rare Move to Stem War Losses," Bloomberg, April 14, 2026, https://www.bloomberg.com/news/articles/2026-04-14/iran-offers-limited-internet-in-rare-move-to-stem-war-losses.