AMERICAN FOREIGN POLICY COUNCIL

IRAN Strategy BRIEF

IRAN'S DIGITAL FORTRESS: THE RISE OF THE NATIONAL INFORMATION NETWORK

CALLA O'NEIL

August 2025 No. 16

While the international community has overwhelmingly focused on Iran's nuclear ambitions and its persistent regional interference, internal political cohesion is an equally important factor in determining the country's future political trajectory. As successive rounds of protests spanning more than two decades have made abundantly clear, the Iranian regime's most acute vulnerability comes not from external attack but from within: from the persistent and growing discontent of its own citizens. In response, Tehran has leaned more and more heavily on a long-term strategy of digital control.

The centerpiece of that effort is a centralized, state-run internet platform known as the National Information Network (NIN). The NIN is portrayed by Iranian officials as a mechanism for cybersecurity and digital sovereignty. In practice, however, it is significantly more. The NIN serves as nothing less than the cornerstone of an emerging model of Iranian authoritarian digital governance.

The purpose of this effort is clear: to curb public dissent, to restrict access to information for Iranians that lies beyond the reach of the country's clerical elites, and to enable comprehensive state surveillance. And as the regime faces threats both from within and from outside of its borders, the NIN has become one of the regime's most powerful tools—not just to manage unrest, but to prevent it in the first place.

THE DIGITAL RESPONSE TO THE JUNE 2025 WAR

The Iranian regime's digital repression reached new heights in June of 2025, when the Islamic Republic initiated a sweeping thirteen-day internet blackout across large parts of the country in response to military action against its nuclear program by Israel and the United States.[1] The shutdown was the most severe since at least 2019, with more than 90 million Iranians taken offline.[2] Analyses show that between June 18th and June 21st, only 1% of monitored IP addresses were functioning within the

Calla O'Neil is a researcher at the American Foreign Policy Council in Washington, DC.

country.[3] The outage blocked communication between friends and family members in Iran, news updates on the conflict from trusted international sources, and social media alerts from the Israeli army warning of strikes.

While the blackout was framed as a national security measure to protect against foreign cyberattacks, the brunt of its impact was felt domestically by civilians, sparking panic and disillusionment among the Iranian public. This policy was not merely a tactical response by the regime to protect Iran in times of war, however. Instead, it is part of a broader campaign of repression by which the Iranian regime has sought to maintain and further strengthen state control. Indeed, alongside the internet blackout, Iranian authorities announced an emergency bill that enables sweeping crackdowns on espionage and dissent, including penalties as severe as capital punishment.[4] Thereafter, around 2,000 arrests were made, with some individuals accused of spying for Israel potentially facing the death penalty.[5]

These steps underscore Iran's contemporary strategic calculus. As its military and nuclear infrastructure comes under foreign attack, the regime in Tehran is doubling down on domestic repression – turning inward and tightening its grip on any activity perceived as a threat to its power.

THE EVOLUTION OF IRAN'S DIGITAL REPRESSION

The digital repression witnessed in June 2025 finds its roots some two decades earlier, as the Islamic Republic belatedly adapted to the fundamentally new set of challenges posed by the advent of large-scale internet access within its borders. Since its founding as a result of the 1979 Revolution, Iran's clerical regime had prioritized suppressing dissent and tightly controlling the flow of information in and out of the country. Yet by the early 2000s, the expansion of digital connectivity had begun to erode that control.

The numbers tell the story. In the year 2000, there were approximately 625,000 internet users in Iran. By 2005, that figure had grown almost ten-fold.[6] And as the Iranian populace increasingly went online, the opportunities for discourse and mobilization expanded as well, while regime control atrophied.

The effects were on display in 2009 during the "Green Movement" that followed the controversial victory of Mahmoud Ahmadinejad in a heavily contested presidential election.[7] Protestors utilized services like Facebook, Twitter, and SMS messaging to organize demonstrations and document instances of police brutality. In response, regime authorities began implementing methods of censorship and surveillance aimed at safeguarding their grip on power. They blocked access to Facebook and Twitter, blocked IP traffic based on select keywords, and throttled internet speeds.[8] Their efforts, however, were only partially successful due to the widespread use of virtual private networks (VPNs), which allowed citizens to circumvent restrictions and highlighted the limits of the state's digital toolkit at the time.

Protests in December 2017 further tested the regime's control of the digital space. Demonstrations were held across the country, catalyzed by economic frustration and disappointment in the "reformist" government then in power. Once again, digital tools, particularly Telegram, proved central to protest coordination, with an estimated 40 million Iranians using the platform to share messages and videos.[9] Authorities ordered the widespread blockage of Telegram, Instagram, and Facebook Messenger across major Iranian Internet Service Providers (ISPs), which led

to spikes in the usage of VPNs and the Tor anonymous browser network—steps that allowed protesters to remain connected to one another and to the international community despite national restrictions.

By November 2019, the regime began to demonstrate significant progress toward total digital control. Faced with renewed nationwide unrest, this time over fuel price hikes, the regime initiated an unprecedented internet blackout. Starting on November 15th of that year, Iranians experienced a complete disconnection of ISPs, isolating the country and silencing protests for nearly a week. The move, enabled in large part by years of investment in the NIN, allowed the regime to obscure its crackdown, limiting the information available to the public regarding the use of deadly force by security forces that killed at least 323 Iranians over five days of protest.[10] This blackout set a new benchmark by the Iranian regime, shifting its strategy from reactive censorship to digital isolation.

Subsequent protests, including the widespread "Woman, Life, Freedom" demonstrations that erupted following the 2022 death of Kurdish-Iranian activist Mahsa Amini while in police custody, have met similar responses.[11] The June 2025 blackout now stands as the latest example of the regime's maturing digital warfare capabilities. Each new wave of unrest has been countered with escalating efforts to disrupt internet access and limit external visibility, illuminating the NIN as both a shield against foreign influence and a weapon against domestic opposition.

AN INFRASTRUCTURE OF ISOLATION

The idea for a national internet network in Iran was first developed by the country's Ministry of Information and Communication Technology (ICT) in 2005.[12] The proposal gained traction in the aftermath of the 2009 "Green Movement," as foreign platforms like Twitter and Facebook made mass mobilization against the regime both feasible and successful. Authorities began laying the groundwork for what was marketed as a "Halal Internet": a sanitized, state-supervised alternative to the global internet that would prohibit access to foreign platforms and replace them with domestic alternatives.[13] By 2012, this concept had evolved into a full national infrastructure project.

Now known as the NIN, Iran's domestic internet functions alongside the global internet, enabling the government to cut off access to the outside world while ensuring the continuance of critical domestic services such as banking, healthcare, and government communications. This parallel system has dramatically reduced the economic and administrative costs previously associated with internet shutdowns. Estimates suggest that a total internet shutdown without the NIN would cost Iran $370 million per day.[14] With the domestic network separated from the global network, however, a blackout to target methods of communication and protest becomes both financially and logistically feasible.

Officially, the NIN serves as a strategic asset that defends against external threats and preserves national sovereignty. It aims to provide users with "safe" content that is "compatible with religious and revolutionary values."[15] Left unsaid in the regime's narrative is the ease with which officials can control information, monitor online activities, and surveil citizens. Additionally, the regime can cut off public internet access without affecting the work of the state or affiliated businesses.

Construction of the NIN formally began in 2013. Since then, at least $6 billion has been invested into domestic digital

infrastructure.[16] The regime has rolled out several homegrown alternatives to international platforms, including "Souroush" as a substitute for Telegram, "Parsijooh" as an alternative search engine, and "Aparat" to replace video streaming platform YouTube. These services are marketed with incentives such as faster speeds and lower data costs, but their true utility lies in offering the regime control over online content and user behavior—capabilities that are absent when Iranians utilize foreign platforms.

The NIN's operational value was first displayed during the 2019 protests, when the regime shut down the global web while leaving local alternatives online. According to one report, around 95% of all internet users were offline within 24 hours of the shutdown, the exceptions being the domestic services used by the government and some public universities.[17] The lesson was clear: the Islamic Republic now possesses the tools to isolate its population while preserving its own digital needs.

IRAN'S GLOBAL PARTNERSHIPS

It should be noted that the Iranian national internet project is not unique. While the details vary, other repressive regimes are also working to erect their own alternatives to the World-Wide Web, and thereby to curate the digital reality of their citizens. And as Iran intensifies its grip over the digital domain, it is drawing from, and aligning with, an emerging coalition of authoritarian powers that have spent the past decade or more perfecting the tools of digital repression.

Russia, for instance, began its campaign to insulate its own information space from foreign influence in 2012.[18] Since then, authorities in Moscow have blocked access to more than 247,000 websites under the guise of targeting "illegal content." Additionally, Russia's creation of distinct domestic internet infrastructure, dubbed RuNet, is nearing operational capacity. In December 2024, several regions across Russia experienced internet disruptions as part of a test period for this national internet system.[19] Despite official claims that the tests were essential in order to guarantee that the domestic network can function independently in the face of foreign threats, human rights groups are increasingly concerned that full implementation of the RuNet could completely isolate Russians from global online platforms and news outlets.[20]

China, meanwhile, has developed its own advanced internet policing capabilities. Since the launch of its Golden Shield project, colloquially known as the Great Firewall, in the late 1990s, Beijing has built a highly sophisticated internet surveillance architecture that leverages IP blocking, keyword filtering, and deep packet inspection to restrict access to information.[21] Today, more than 311,000 domains are blocked daily within China.[22] Over time, the Chinese model has evolved far beyond content restriction to include the identification and tracking of internet users. Individuals have to complete identity checks on every online platform, including the highly popular Chinese messaging app WeChat, making it nearly impossible for users to remain anonymous.[23] Moreover, China's surveillance capabilities extend beyond private networks to public Wi-Fi access points in airports, hotels, and malls.[24] Nor is China a stranger to utilizing internet blackouts; in 2009, authorities imposed a 10-month blackout on Xinjiang following deadly ethnic riots in that region.[25]

The Islamic Republic has been a beneficiary of Chinese and Russian surveillance expertise for nearly two decades. Chinese tech giants like Huawei Tech-

nologies and ZTE Corp have supplied Iran with the hardware and infrastructure needed to monitor its population at scale. In 2009, Huawei and British company Creativity Software supplied MTN Irancell, one of Iran's largest mobile phone carriers, with a system that can be used to track the locations of its users.[26] One year later, ZTE signed a deal with Iran's largest telecom firm to supply a system with capabilities to locate users and intercept voice calls, text messaging, email, chat conversations, and web access.[27]

Today, that cooperation is entering a new phase. In January 2025, Tehran and Moscow signed a deal to, among other things, increase collaboration on cybersecurity and internet regulation.[28] Though specifics remain opaque, discussions from a 2023 meeting between the Russian and Iranian technology ministries suggest that this partnership could include the export of Russian technologies to Iran.[29]

Similarly, Tehran is deepening its ties with Beijing. In May, Iranian information and communication technology officials met with their Chinese counterparts to discuss expanding cooperation into artificial intelligence (AI), industrial intelligence, and the development of communications infrastructure.[30]

This tightening nexus of cooperation is about more than technology; it represents a coordinated effort to combat Western influence in the digital space and eliminate the norms of internet freedom that empower citizens to use their voices against their governments.

TIGHTENING THE DIGITAL CAGE

Notably, Iran's struggle to eliminate VPN usage remains a significant obstacle to the expansion of NIN capabilities. While all major social media applications, including Instagram, Twitter, YouTube, and Telegram, are officially banned in Iran, alongside thousands of websites,[31] these platforms remain highly popular for millions of Iranians thanks to encrypted connections that allow users to circumvent government controls. This practice has birthed a major market in Iran, with nearly 87% of Iranian users relying on subscription-based VPNs.[32] Estimates place the VPN market in Iran at exceeding $85 million annually—a direct reflection of public defiance and a persistent reminder of the present technological limitations of the NIN.

In response, Iranian authorities have intensified efforts to assert control. In 2022, the regime criminalized the sale and distribution of VPNs.[33] More recently, in February 2024, the country's Supreme Council of Cyberspace (SCC) issued a sweeping directive forbidding the use of "refinement-breaking tools" without the presence of a legal permit.[34] The mandate sparked immediate backlash, prompting SCC Secretary Mohammad Amin Aghamiri to clarify a day later that the regulations apply solely to state institutions, not the general public.

The February directive included additional guidance that will guide the development of the NIN for the foreseeable future. First, the Culture Ministry is to collaborate with the Economic and ICT Ministries to come up with a plan to incentivize content creators and businesses active on foreign platforms to fully switch over to local platforms. The goal was to bring at least half of the target audience to local platforms within six months. This focus is telling; polling conducted in May 2024 by the Iranian Students Polling Agency indicates that usage of international platforms still significantly outweighs that of domestic platforms.[35]

Another facet of the regime's strategy is the development of "shell" versions of

international applications. These modified clones would offer Iranians access to familiar interfaces that would not be blocked like the main versions. However, foreign platforms would have to adhere to Iranian rules in order to create a "governable format," including placing representatives in Iran that are accountable to the clerical state.[36] So far, no international company has agreed to these terms.

In August 2024, Supreme Leader Ali Khamenei called upon newly elected President Masoud Pezeshkian to enact greater restrictions on what he termed the "uncontrolled" state of Iran's internet. Pezeshkian, who criticized internet filtering during his presidential campaign due to its negative impact on the economy, has changed his tune and is now calling for the SCC to implement tighter controls over cyberspace, signaling a broad regime commitment to digital autarky. Moreover, the regime appears to be making progress toward this goal. According to Communications Minister Sattar Hashemi, roughly 60% of NIN's infrastructure is now operational. However, the true state of the NIN remains unclear.

In parallel with the expansion of the NIN, the Iranian regime is turning to next-generation technologies as new instruments of repression. In March of this year, authorities unveiled a prototype for a national artificial intelligence platform, with plans for a nationwide rollout by March of 2026.[39] Positioned as a strategic move in the global "war of chips and algorithms," the initiative reflects a critical step toward reducing dependency on foreign platforms and reinforcing the regime's burgeoning architecture of domestic control. Beyond this AI platform, Iran has already integrated facial recognition into public surveillance systems and harnessed machine learning to monitor social media activity for dissent. Increasingly, in other words, the regime is positioning itself as an authoritarian government capable of withstanding the digital age.[40]

TOWARD A CLOSED IRANIAN INTERNET

The recent war with Israel has assuredly further incentivized Iran's efforts to assert total digital control. With the regime's strategic credibility now under heightened scrutiny, the Islamic Republic will continue to pour resources into what it has come to see as a crucial line of defense: control over its captive population. And once fully realized, the NIN will grant the Iranian regime unprecedented ability to sever international connectivity without disrupting core domestic infrastructure.

Government-mandated internet shutdowns, like those conducted by Iranian authorities in the past, have been condemned by the United Nations as violations of human rights.[41] Real consequences for such disruptions, however, have been overwhelmingly absent to date. That is assuredly instructive for Iran's regime. As it pushes the boundaries of acceptable behavior in cyberspace, the Islamic Republic has become emboldened by the lack of consequence so far—and by the assumption that it will continue to avoid significant punishment in the future.

Additionally, sanctions levied on the regime by the United States have provided it with justification of sorts for the NIN. 2010 sanctions preventing U.S. companies from hosting ".ir" domains forced Iranian organizations to host their websites domestically. Furthermore, President Trump's "maximum pressure" strategy against Iran has aided the official rhetoric surrounding the NIN, allowing authorities to frame it not as a tool of oppression but as a part of Iran's anti-imperialist struggle against the West.[42] By further fueling Iran's iso-

lationist mentality, the perceived necessity of the NIN increases, inching the regime closer to complete isolation from the outside world.

An Iran that is fully isolated digitally would further impoverish the country's shrinking civil society space, cutting off access to global information flows and preventing the documentation of state abuses. While the regime may view increased censorship as a pathway to greater political stability, history suggests that Iranian dissent is both adaptive and persistent. From VPN usage to creative workarounds like using the traffic app Waze for protest coordination, the Iranian people have repeatedly demonstrated a capacity to outmaneuver state controls.[43] Nevertheless, the NIN clearly represents a significant evolution in Iran's authoritarian toolkit.

ENDNOTES

1. Deepa Parent, "'It's like being walled in': young Iranians try to break through internet blackout," *The Guardian*, June 25, 2025, https://www.theguardian.com/world/2025/jun/25/young-iranians-break-through-internet-blackout.
2. "Internet blackout in Iran: RSF condemns the information blackout orchestrated by the regime amid war with Israel," Reporters Without Borders, June 20, 2025, https://rsf.org/en/internet-blackout-iran-rsf-condemns-information-blackout-orchestrated-regime-amid-war-israel.
3. "Iran has come back online—for now," *The Economist*, June 26, 2025, https://www.economist.com/graphic-detail/2025/06/26/iran-has-come-back-online-for-now.
4. Susannah George, "Iranian authorities make sweeping arrests in wake of war with Israel," *Washington Post*, July 1, 2025, https://www.washingtonpost.com/world/2025/07/01/iran-israel-conflict-arrests/.
5. "Iran detains 2,000 in war sweep, some may face death for Israel espionage," *Iran International*, July 23, 2025, https://www.iranintl.com/en/202507220323.
6. Michael Rubin, "Evolution of Iranian Surveillance Strategies Toward the Internet and Social Media," American Enterprise Institute, January 3, 2018, https://www.voanews.com/a/difference-between-2009-and-2018-iran-protests-is-48-million-smartphones-/4190712.html.
7. Hamid Dabashi, "What happened to the Green Movement in Iran?" *Al-Jazeera*, June 12, 2013, https://www.aljazeera.com/opinions/2013/6/12/what-happened-to-the-green-movement-in-iran.
8. Sean A. Williams, "Iranian National Information Network," Air Command and Staff College Air University, December 2019, https://apps.dtic.mil/sti/pdfs/AD1107324.pdf.
9. Ibid.
10. A Web of Impunity: the Killings Iran's Internet Shutdown Hid," Amnesty International, n.d., https://iran-shutdown.amnesty.org/.
11. Azadeh Akbari, "Shutting down the internet is another brutal blow against women by the Iranian regime," *The Guardian*, September 26, 2022, https://www.theguardian.com/commentisfree/2022/sep/26/elon-musk-iran-women-mahsa-amini-feminists-morality-police.
12. Dipayan Ghosh, "The Isolating Effects of Iran's Proposed 'National Internet,'" Centre for International Governance Innovation, January 27, 2021, https://www.cigionline.org/articles/isolating-effects-irans-proposed-national-internet/.
13. Williams, "Iranian National Information Network."
14. Mahsa Alimardani, "The Ayatollah Comes for the Internet," *New York Times*, November 19, 2019, https://www.nytimes.com/2019/11/19/opinion/iran-internet-ban.html.
15. "Iran's National Information Network," Citizen Lab, November 9, 2012, https://citizenlab.ca/2012/11/irans-national-information-network/.
16. "10 Things You Should Know About Iran's Multi-Billion Dollar National Internet Project," Center for Human Rights in Iran, October 13, 2016, https://iranhumanrights.org/2016/10/ten-things-you-should-know-about-irans-national-internet-project/.
17. Alimardani, "The Ayatollah Comes for the Internet."
18. Daryna Antoniuk, "Russia disrupts internet access in multiple regions to test 'sovereign internet,'" *The Record*, December 9, 2024, https://therecord.media/russia-disrupts-internet-access-in-multiple-regions-runet.
19. Ibid.
20. "Russia: Growing Internet Isolation, Control, Censorship," Human Rights Watch, June 18, 2020, https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.
21. "Free Speech vs Maintaining Social Cohesion: A Close Look at Different Policies," Stanford University, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.

22. Emily Quan, "Censorship Sensing: The Capabilities and Implications of China's Great Firewall Under Xi Jinping," *Sigma: Journal of Political and International Studies* 39, 2022, https://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=1312&context=sigma#:~:text=Focusing%20on%20Narrative%20Control,information%20that%20enters%20its%20borders.
23. John Liu, "China tightens internet controls with new centralized form of virtual ID," *CNN*, June 20, 2025, https://www.cnn.com/2025/06/20/tech/china-censorship-internet-id-hnk-intl.
24. Minxin Pei, "China's Secret to Controlling the Internet," *Foreign Policy*, February 19, 2024, https://foreignpolicy.com/2024/02/18/china-internet-control-ccp-technology-cyber-surveillance-policy-sentinel-state/.
25. Amy Hawkins, "'Alarming' rise in regional internet censorship in China, study finds," *The Guardian*, May 24, 2025, https://www.theguardian.com/world/2025/may/24/alarming-rise-in-regional-internet-censorship-in-china-study-finds.
26. "Special Report – Chinese firm helps Iran spy on citizens," Reuters, March 22, 2012, https://www.reuters.com/article/business/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSL3E8EM4QW/.
27. Ibid.
28. Daryna Antoniuk, "Iran and Russia deepen cyber ties with new agreement," *The Record*, January 22, 2025, https://therecord.media/russia-iran-cyber-ties-agreement.
29. "Tehran's preference: Russia's technological sector offers partnership to Iran [Тегеранская преференция: Технологический сектор России предложил Ирану партнерство]," *Kommersant*, July 7, 2023, https://www.kommersant.ru/doc/6084928.
30. "Iran, China discuss ways to foster technological partnerships," *Tehran Times*, May 14, 2025, https://www.tehrantimes.com/news/513061/Iran-China-discuss-ways-to-foster-technological-partnerships.
31. Maziar Motamedi, "Iran unveils plan for tighter internet rules to promote local platforms," *Al-Jazeera*, February 24, 2024, https://www.aljazeera.com/news/2024/2/24/iran-unveils-plan-for-tighter-internet-rules-to-promote-local-platforms.
32. "The final straw: Iranians dread plans for a 'national' internet," *Iran International*, August 22, 2024, https://www.iranintl.com/en/202408218106.
33. Motamedi, "Iran unveils plan for tighter internet rules to promote local platforms."
34. Ibid.
35. "State-backed poll shows most Iranian students use foreign social media," *Iran International*, October 14, 2024, https://www.iranintl.com/en/202410135352.
36. Motamedi, "Iran unveils plan for tighter internet rules to promote local platforms."
37. Pejman Amiri, "Iran's Escalating Internet Censorship: From Filtering to a National Internet," *Iran News Update*, August 29, 2024, https://irannewsupdate.com/news/general/irans-escalating-internet-censorship-from-filtering-to-a-national-internet.
38. "The Final Straw," *Iran International*.
39. "Iran unveils national AI platform prototype," *Iran International*, March 15, 2025, https://www.iranintl.com/en/202503158253.
40. "Artificial intelligence (AI) and human rights," European Parliament, 2024, https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf.
41. "A Web of Impunity: the Killings Iran's Internet Shutdown Hid."
42. Ryan Grace, "Shatter the web: Internet fragmentation in Iran," Middle East Institute, December 14, 2020, https://www.mei.edu/publications/shatter-web-internet-fragmentation-iran.
43. Alimardani, "The Ayatollah Comes for the Internet."

The American Foreign Policy Council

For more than four decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies.

AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.