



AMERICAN FOREIGN POLICY COUNCIL

PUBLIC DIPLOMACY PAPER

AUGUST 2026 • NO. 1

HIGHLIGHTS

The 88-day blackout in Iran between Feb. 28 and May 26 became the longest nationwide internet shutdown in modern history.

Tehran's strategy in the information space has evolved from blunt, reactive censorship to a more sophisticated model that utilizes selective access, advanced technologies, and heightened attacks on traditional workarounds.

In this latest blackout, the regime exhibited unprecedented legal and technical capabilities to suppress internet use, including new legislation criminalizing Starlink possession and military-grade jamming equipment.

Direct-to-cell (D2C) satellite technology represents a promising solution, but key limitations must be addressed.

PLANNING FOR THE NEXT IRANIAN INTERNET BLACKOUT

CALLA O'NEIL

On February 28, 2026, the day President Trump announced the start of “major combat operations” against the Islamic Republic, Iranian authorities cut all internet access, plunging Iran into what became an 88-day nationwide blackout—the longest in modern history. Regime officials publicly framed the shutdown as a national security imperative. In practice, it halted online commerce, severed the flow of information coming from international news outlets and social media, and cut off citizens from family and friends abroad. As strikes continued against military, government, and at times civilian targets, Iranians were left with only state-authorized websites and news sources, designed to project a

unified, resilient Islamic Republic and silence internal dissent.

Decades of unreliable connectivity have left Iranians well-practiced in circumvention, finding ways to reach the outside world even as Tehran tries to cut them off. But as these tools have advanced, so have the countermeasures the regime deploys to keep its population offline.

As of May 26th, Iranian internet access has been slowly restored, although internet freedom remains far from realized. Users report significantly degraded internet speeds compared to pre-blackout levels, and access to major social media platforms, including Instagram and TikTok, remains heavily restricted even through VPN services. With connectivity still in flux, the best

Calla O'Neil is a Research Fellow and Program Officer at the American Foreign Policy Council.

defense against Tehran's next censorship campaign lies in the lessons accumulated from this blackout: how the regime adapted to sophisticated circumvention tools, and how those tools must evolve to withstand harsher restrictions going forward.

A BRIEF HISTORY OF IRANIAN INTERNET CONTROL

While the Spring 2026 shutdown may have been the longest Iranians have been offline, it is certainly not the first time. Ever since the internet first proved useful for Iranians to communicate and mobilize—in particular, against the regime—the Islamic Republic has worked assiduously to restrict it.

The first instance of mass censorship came in 2009, when three million Iranians took to the streets to protest the controversial victory of presidential candidate Mahmoud Ahmadinejad in what became known as the Green Movement.² Protesters used Facebook, Twitter, and SMS to organize demonstrations and document police violence against them.³ Tehran adapted in real time: blocking Facebook and Twitter, filtering IP traffic based on keywords, and throttling internet speeds.⁴ But widespread access to virtual private networks (VPNs) let Iranians reach restricted platforms through remote servers.⁵

The Islamic Republic has since expanded its digital toolkit to prevent these workarounds. By November 2019, authorities carried out Iran's first true internet blackout—a total disconnection of internet service providers (ISPs) rather than selective platform or keyword blocking. This marked a shift from reactive censorship to full digital isolation.⁶ Since then, there have been four major nationwide blackouts, including the most recent, which occurred from February 28th to May 26th of this year.

Tehran has also built out domestic internet infrastructure to tighten its control over the flow of information. Since 2013, the regime has invested at least \$6 billion in the National Information Network (NIN), a tightly controlled domestic internet that could remain functioning even when authorities cut off global internet access. The NIN includes domestic alternatives to popular platforms like Telegram, Google, and YouTube, laying the groundwork for an internet environment fully sealed off from the international community and monitored by Iranian authorities.⁷

The Islamic Republic's surveillance capabilities have expanded alongside this infrastructure. In 2023, the regime announced the expansion of CCTV coverage, including on public transit and in apartment complexes, to monitor dissent and noncompliance with the hijab mandate.⁸ A year later, the regime's Seventh Development Plan introduced the "Lifestyle Assessment System," which tracks citizens' travel, shopping, and financial activities data onto a single digital platform shared across government bodies.⁹

Yet despite internet shutdowns, the NIN, and expanding surveillance, Iranians have persistently found ways to stay connected. For over a decade, VPNs have been the primary tool for bypassing censorship and reducing surveillance risks.¹⁰ A 2025 survey found that 81 percent of Iranians relied on VPNs for these purposes.¹¹ Iranians have also increasingly turned to Starlink, SpaceX's network of low-orbit satellites, which allows users to bypass the terrestrial internet entirely.¹² An estimated 50,000 Starlink terminals operate in Iran, connecting roughly 100,000 Iranians to uncensored internet.¹³ Yet the latest shutdown exposed the limitations of these tools. A reassessment of how to keep Iranians online during conflict and unrest is therefore needed.

CONNECTIVITY IN A TIME OF WAR

The latest internet shutdown—coinciding with the war between Iran, Israel, and the United States—exhibited the most sophisticated censorship crackdown in Iranian history.

Throughout the blackout, connectivity held at roughly 1 percent of pre-conflict levels.¹⁴ By April 21st, the blackout's 53rd day, it had become the longest nationwide internet outage in modern history.¹⁵ The economic costs were significant for an Iranian economy already floundering through war: an estimated \$35-40 million in direct losses accumulated daily, small businesses reliant on internet access collapsed, and millions of workers were affected.¹⁶ Moreover, in a recent survey, when Iranian civilians were asked about the economic consequences of the internet shutdown on their households, 35.5 percent reported an "increase in living costs," 29 percent reported a "decrease in income," and 76 percent cited "high prices, inflation, and economic pressure" as their primary concern during the war.¹⁷

The humanitarian cost was equally stark. Hospital staff, cut off from reliable communication, reported

critical shortages of blood and medical supplies and an inability to coordinate emergency care or telemedicine.¹⁸

Not all Iranians faced these conditions equally, however. On April 22nd, roughly a month into the blackout, Iran's National Security Council introduced "Internet Pro," a tiered access system. At the highest tier, a preapproved digital elite could purchase unrestricted "white SIM cards" granting full global internet access.¹⁹ Meanwhile, lower tiers offered limited connectivity with filters and daily limits at a fixed cost per gigabyte—effectively converting the information space into a class-based system.²⁰ Unlike VPNs, which bypass censorship by encrypting traffic, Internet Pro routed approved users through less restricted gateways. Regime spokeswoman Fatemeh Mohajerani confirmed that access was selectively granted to "those who can better deliver the message"—that is, key officials, businesses, and pro-regime influencers who continued posting freely on social media while the rest of the Iranian population remained silenced.²¹

Tehran simultaneously moved to suppress the circumvention tools Iranians have long relied on during periods of digital disruption. Authorities enforced 2025 legislation criminalizing satellite internet use, including Starlink: possession, purchase, or sale of unauthorized terminals now carries a six-month to two-year prison sentence, while manufacturing or importing more than ten devices carries a jail term of five to ten years.²²

The human toll of this legislation became evident this spring. At least 100 people were arrested for terminal possession during the blackout, and over 400 for using the internet "to hurt national security."²³ In May, Hesam Alaeddin, a 40-year-old detainee arrested for using Starlink, died in custody in Tehran after being severely beaten by government agents.²⁴ Authorities also arrested two foreign nationals for allegedly importing satellite equipment.²⁵

Alongside these scaled up arrests, the Islamic Republic further cracked down on Starlink usage, deploying military-grade electronic equipment (mirroring technology employed by Russia in Ukraine) to jam Starlink signals.²⁶ Additionally, the regime flew drones over rooftops to locate Starlink satellite dishes and publicized terminal confiscations to spread fear.²⁷

Authorities also pressured civilians into flooding their own social media feeds with pro-regime content. Multiple outlets reported that Iranians seeking restored access were ordered to surrender personal information

—home addresses, bank account information, pictures of their bank cards, and links to their social media accounts—and to sign handwritten pledges not to publish content harmful to Iran's "psychological, social, or political security," with some required to publish at least 20 pro-regime posts to their social media feeds.²⁸ By enticing Iranians desperate to reach their loved ones and sustain their livelihoods with restored connectivity, the regime worked to project internal cohesion by populating the information space with propaganda.

NEW AND OLD WORKAROUNDS

Selective internet access, a crackdown on circumvention tools, and pro-regime propaganda together defined the regime's latest bid to keep Iranians offline and isolated. Facing its most advanced shutdown yet, Iranians turned to both old and new methods to get online, albeit with mixed results.

Psiphon Conduit: Diaspora-enabled internet

During the latest shutdown, Iranians turned to relay tools built by VPN companies that enabled encrypted peer-to-peer connections—allowing individuals outside Iran to share open internet access with those inside facing censorship. A popular service run by the VPN company Psiphon is called Psiphon Conduit. When an Iranian user connects through Psiphon, their traffic routes through a Conduit Station on an external volunteer's device, then forwards to Psiphon's servers.²⁹ Iranian authorities have grown increasingly able to identify and block users who connect to the standard Psiphon VPN server. But by routing through external volunteers' devices, each connected to its own home WiFi network, Iranians can access the open internet without relying on a fixed set of server addresses that the regime can catalog and block. Each external user can enable access for roughly 25 people, though speeds can be unreliable.

Diaspora Iranians with unrestricted internet access have widely installed Psiphon Conduit and similar tools, such as Tor's Snowflake project.³⁰ Iran now has more Psiphon users than any other country in the world, and at the height of the internet disruption Psiphon was recording as many as 26 million daily connections from Iran.³¹

However, Psiphon Conduit shares a fundamental limitation with traditional VPNs. During a true nationwide blackout, when a regime severs all international

routes or forces traffic onto a closed national network, no VPN tool can function. These tools can encrypt and reroute traffic, but they cannot create a path to the global internet where none exists. Therefore, Iranians could not connect using Conduit for the first month of the blackout, until Internet Pro began slowly introducing pathways to external addresses. Amnezia, another VPN historically used during internet blackouts, suffered the same collapse—its nearly 300,000 users in Iran dropped to almost zero once the blackout took hold.³²

The shutdown also created an opening for fraudulent VPN services, reportedly tied to Iranian state actors.³³ VPNs using the .ir domain have emerged, with some configurations failing to encrypt traffic at all and exposing users' browsing behavior and destinations.³⁴

Starlink

Starlink's advantage over VPNs is that satellite-initiated internet can function even when the terrestrial internet is disrupted, relying instead on a constellation of low-Earth orbit satellites.

Starlink's constellation comprises 10,365 satellites, roughly two-thirds of all active satellites around the world.³⁵ An estimated 50,000 Starlink terminals are reportedly active in Iran,³⁶ in addition to a reported shipment of 6,000 Starlink terminals provided by the Trump administration following the regime's brutal crackdown on January's demonstrations.³⁷

However, Starlink has not delivered the disruption-free internet service Iranians hoped for. While the regime's previous strategy of disrupting Starlink connectivity through GPS jamming had only limited success, the latest blackout saw the deployment of new, more powerful military-grade jamming tools that degraded the connection severely enough to block images and videos from being shared.³⁸ Experts indicate that these jamming systems are either domestically produced or made with equipment sourced from Russia or China.³⁹ Starlink connections were also reported as unstable, slow, and unreliable, to the point of barely functioning during the blackout.⁴⁰ Criminalized possession of Starlink terminals also made it difficult to smuggle terminals across Iranian borders and heightened the risk of users being identified through government geolocators.⁴¹ The terminals' high price tag (smuggled terminals on the black market have reportedly soared to as much as \$4,000 apiece⁴²) further undermines its viability as a sustainable, scalable solution.

Crossing borders

Beyond circumvention tools, some Iranians have resorted to crossing borders to reach the internet. Reports indicate Iranians traveled into Turkey and Iraq during the war to get online and contact loved ones.⁴³ In border communities, Iraqi mobile network SIM cards—which carry partial coverage into Iran's frontier areas—gained particular traction.⁴⁴ As Iranians began identifying the strongest cross-border reception points, people began flocking to these areas to call relatives or manage online businesses. But even this workaround carried serious risk; for instance, shortly after Iranians began gathering near Baneh, a city close to the Iraqi border, to access stronger cell service, authorities raided the site, arresting more than 50 people and confiscating their phones.⁴⁵

WHERE WE ARE TODAY

Since May 26th, internet access has been gradually returning. The restoration followed a vote by the Special Task Force on Cyberspace Management, which President Masoud Pezeshkian appointed earlier that month to resolve “conflicting voices” over cyberspace policy amid popular frustration. On May 25th, task force members voted nine to two in favor of restoring access, and Minister of Communications Sattar Hashemi announced the following day that the reinstatement process had begun.⁴⁶

Accessing the global internet through VPNs is now possible, but Iran's internet is still far from free. Millions of websites remain blocked and nearly all global platforms including YouTube, Instagram, Telegram, WhatsApp, Facebook, and Waze remain inaccessible. Mobile, wireless, and landline connections are slow and inconsistent, and even unblocked foreign IP addresses are difficult to reach given that authorities have only permitted a limited volume of traffic and data packets.⁴⁷

Even so, the decision to reopen was far from unanimous among the Iranian leadership. Several members of the Supreme National Security Council and other state bodies even attempted to halt the reopening entirely, petitioning the Administrative Court of Justice to suspend the Special Task Force and its orders.⁴⁸ Given this hardliner resistance, the future of restored internet access, however limited, remains uncertain. As such, it is high time to focus on alternatives capable of bypassing total national shutdowns.

LOOKING AHEAD

Direct-to-cell (D2C) technology offers one such alternative. Rather than requiring a physical terminal, D2C connects ordinary phones directly to satellites in space, eliminating the security risk of smuggling and storing hardware inside Iran. It would also remove the financial barrier that has limited access to those who can afford a terminal; most smartphones manufactured since 2020 already have the technical foundation for D2C connectivity built in.⁴⁹

Major satellite operators—including SpaceX, AST SpaceMobile, and Globalstar—have deployed low-Earth orbit satellites that function as cell towers in space. D2C requires a partnership with a mobile network operator (MNO), which licenses its spectrum to the satellite company, extending coverage beyond the operator's existing coverage. If a MNO designates Iranian territory as an uncovered zone included in its service, any phone using that operator's SIM or eSIM could establish a D2C connection from inside Iran to these satellites.⁵⁰

Several MNOs, including T-Mobile, KDDI, and One NZ, have partnered with satellite providers to launch D2C services aimed at covering traditional mobile dead zones.⁵¹ But the technology is not yet ready for use at scale in Iran. First, D2C is designed for emergency coverage in low or no-coverage areas, not as a substitute for national internet infrastructure. A city like Tehran, where millions would need simultaneous access to messaging, maps, email, and financial services, would demand far greater network capacity than currently exists.

Second, D2C currently carries a risk of radio interference and exposure. The regime could manipulate the domestic radio environment—mobile towers, ground transmitters, and local signals—to overpower the comparatively weak signal coming from satellites positioned above Earth, thereby disrupting connections. Additionally, because authorities can link a phone's serial number to the user's identity, activating a foreign SIM on a registered device to reach a satellite network could be flagged and trigger surveillance. To implement this technology in Iran, D2C operators need to address these vulnerabilities and ensure that connections remain both strong and untraceable.

Nevertheless, the appeal of this technology is clear: it would eliminate the cost and risk of procuring Starlink hardware and remain functional even during total internet shutdowns, when VPN encryption becomes

irrelevant. But limited capacity and unresolved security risks mean it is not yet a viable solution.

Iran's latest internet blackout offers a sobering lesson: Tehran's censorship strategy has evolved beyond reactive suppression. Once reliant on blunt instruments like blocking platforms and cutting off ISPs entirely, the regime now pairs total shutdown capability with mechanisms to selectively reopen access on its own terms. This shift has exposed the limits of existing circumvention tools. VPN-based services like Psiphon Conduit and Amnezia depend on an underlying path to the global internet, so when Tehran severed that path entirely, these tools collapsed to near-zero functionality. Starlink, which emerged as the more promising solution, could function in principle during the terrestrial blackout, but remained vulnerable to military-grade jamming and criminal persecution under new legislation.

The implications are clear. No tool currently at our disposal can withstand Iran's censorship apparatus indefinitely. An innovative, layered approach must be developed and stress-tested before the next shutdown, rather than improvised during it.

Here, the United States has an important role to play. First, human rights and internet freedom must be built into any future agreement between Washington and Tehran. The now-abandoned memorandum of understanding released on June 14th imposed a 60-day ceasefire and outlined a 14-point framework for a formal agreement, albeit absent any provision on civil liberties.⁵² As of July 7th, strikes have resumed and President Trump has declared the ceasefire over.⁵³ As the Trump administration reconsiders what a future deal could look like, human rights must be prioritized alongside reopening the Strait of Hormuz and establishing a sustainable nuclear framework, so as to ensure that the Iranian people are not left behind.

Simultaneously, the United States should pursue targeted efforts to build up internet freedom infrastructure. Legislation like the *Iran Human Rights, Internet Freedom, and Accountability Act* currently before the Senate offers a mechanism to advance human rights in Iran independent of any bilateral agreement. The bill would mandate an assessment of D2C's feasibility for expanding Iranian internet access and support the development of "low-cost, easily scalable, and rapidly deployable technologies to counter

internet shutdowns.”⁵⁴ It would also raise annual funding for the Iran Internet Freedom Grant Program to at least \$20 million for the next three years, establishing a clear pathway for circumvention tool development.

The stakes are high. Tehran will apply the lessons of its latest blackout to refine the next one. It is up to the United States to apply them as well by investing today in scalable, resilient technologies, so that the next time the Islamic Republic moves to isolate its population from the world, Iranians have the tools they need to stay connected. ♦♦

ENDOTES

1. Omid Habbinia, “Postwar Internet in Iran: More Censorship and Greater Risks for Users,” *The Media Line*, July 9, 2026, <https://themedialine.org/top-stories/post-war-internet-in-iran-more-censorship-and-greater-risks-for-users/>.
2. Abbas Milani, “Iran Primer: The Green Movement,” *PBS*, October 27, 2010, <https://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/10/iran-primer-the-green-movement.html>.
3. Calla O’Neil, “Iran’s Digital Fortress: The Rise of the National Information Network,” American Foreign Policy Council *Iran Strategy Brief* no. 16, August 4, 2025, <https://www.afpc.org/publications/policy-papers/irans-digital-fortress-the-rise-of-the-national-information-network>.
4. Ibid.
5. Ibidem.
6. Ibidem.
7. O’Neil, “Iran’s Digital Fortress: The Rise of the National Information Network.”
8. “Sadar Radan: Coverage of security cameras will increase to ensure public security,” *Fars News Agency*, June 15, 2023, <https://farsnews.ir/Provinces/1686835179000313655/%D8%B3%D8%B1%D8%AF%D8%A7%D8%B1->
9. Louis Shakibi, “How the Iranian Parliament Plans to Spy on Citizens with the ‘Lifestyle Assessment System,’” *Filter Watch*, October 30, 2023, <https://filter.watch/english/2023/10/30/policy-monitor-oct-2023/>.
10. Zvika Klein, “Iranian People Use VPNs to Fight the Regime with Internet Connectivity,” *Jerusalem Post*, January 1, 2026, <https://www.jpost.com/opinion/article-882089>.
11. “81% of Iranian Internet Users Bypass Censorship with VPNs - Parliament,” *Iran International*, February 24, 2025, <https://www.iranintl.com/en/202502243980>.
12. Karl Vick, “Receivers for Elon Musk’s Starlink Internet Are Being Smuggled Into Iran,” *TIME*, October 22, 2022, <https://time.com/6223999/starlink-iran-elon-musk/>.
13. Adam Santariano, Paul Mozur, and Sheera Frenkel, “How Activists in Iran Are Using Starlink to Stay Online,” *New York Times*, January 15, 2026, <https://www.nytimes.com/2026/01/15/technology/iran-online-starlink.html>.
14. Maziar Motamedi, “Frustration Grows as Iran’s Wartime Internet Shutdown Breaks Grim Record,” *Al Jazeera*, April 5, 2026, <https://www.aljazeera.com/news/2026/4/5/frustration-grows-as-irans-wartime-internet-shutdown-breaks-grim-record>.
15. Henna Moussavi, “The Longest Internet Blackout in History Is Crippling Iran’s Economy,” *Wall Street Journal*, May 20, 2026, <https://www.wsj.com/world/middle-east/the-longest-internet-blackout-in-history-is-crippling-irans-economy-0f2d0091>.
16. Maryam Sinaiee, “Iran’s Digital Economy Battered by Prolonged Blackout,” *Iran International*, April 14, 2026, <https://www.iranintl.com/en/202604149190>.
17. Maleki, Ammar. “Iranians’ Attitudes Toward the 2026 Protests and War.” The Group for Analyzing and Measuring Attitudes in Iran (GAMAAN), July 2026, 19–20, <https://gamaan.org/wp-content/uploads/2026/07/GAMAAN-2026-Protests-and-War-Survey-Report-Final-English.pdf>.
18. Mohammad Karamouzian and Stefan D Baral, “Internet Shutdowns in Iran and the Right to Health,” *The Lancet* 407, no. 10531, February 28, 2026, 847–48, [https://doi.org/10.1016/s0140-6736\(26\)00215-1](https://doi.org/10.1016/s0140-6736(26)00215-1).
19. Tim Lister and Aida Karimi, “Iran’s Two-Tier Internet Access Fuels Anger and Exposes Cracks in the Regime,” *CNN*, May 10, 2026, <https://www.cnn.com/2026/05/10/middleeast/iran-internet-pro-blackout-access-vpn-intl>.
20. Negar Mojtahedi, “Internet Pro or Censor Pro? Iran Rolls out a New Service,” *Iran International*, April 22, 2026, <https://www.iranintl.com/en/202604225630>.
21. “Iran Keeps Loyal Voices Online as Public Faces Record Internet Blackout,” *Iran International*, March 10, 2026, <https://www.iranintl.com/en/202603106004>.
22. “Iran Criminalizes Starlink Use, Imposes Death Penalty for Ties to Israel,” *Iran Wire*, July 1, 2025, <https://iranwire.com/en/news/142856-iran-criminalizes-starlink-use-imposes-death-penalty-for-ties-to-israel/>.
23. Emily Feng, “Iranians Are Leaving the Country Just to Access the Internet,” *NPR*, April 22, 2026, <https://www.npr.org/2026/04/22/g-s1-118339/iran-internet-access-turkey>.
24. “Man Arrested for Using Starlink Dies after Beating by Iran Security Forces,” *Iran International*, May 1, 2026, <https://www.iranintl.com/en/202605018963>.
25. “Two Foreigners Arrested in Iran for Importing Starlink Technology, Tasnim Reports,” *Reuters*, April 19, 2026, <https://www.reuters.com/world/middle-east/two-foreigners-arrested-iran-importing-starlink-technology-tasnim-reports-2026-04-19/>.
26. Dinah van der Geest, “What Iran’s Internet Shutdown Reveals about Starlink,” *Tech Policy Press*, February 5, 2026, <https://www.techpolicy.press/what-irans-internet-shutdown-reveals->

- [about-starlink/](#); “Iran Uses Electronic Warfare to Disrupt Starlink — NYT,” *Iran International*, January 16, 2026, <https://www.iranintl.com/en/202601165377>.
27. Santariano, Mozur, and Frenkel, “How Activists in Iran Are Using Starlink to Stay Online.”
 28. Saba Heidarkhani, “Iranians Told to Post Pro-Government Content to Regain Internet Access,” *Iran International*, March 12, 2026, <https://www.iranintl.com/en/202605129643>.
 29. “Frequently Asked Questions (FAQ),” Conduit, from Psiphon, n.d., <https://conduit.psiphon.ca/>.
 30. Maryam Sinaiee, “Volunteers Abroad Deploy Tech to Pierce Iran’s Internet Iron Curtain,” *Iran International*, January 27, 2026, <https://www.iranintl.com/en/202601240957>.
 31. Ibid; Chiara Castro, “‘Iranians Are Resilient; They Always Find Ways to Speak’: How Iranians Are Overcoming Unprecedented Internet Censorship,” *TechRadar*, February 20, 2026, <https://www.techradar.com/vpn/vpn-privacy-security/iranians-are-resilient-they-always-find-ways-to-speak-how-iranians-are-overcoming-unprecedented-internet-censorship>.
 32. “Internet Censorship in Iran: Trends and Outlook for 2026,” *Amnezia*, May 14, 2026, <https://amnezia.org/blog/internet-censorship-in-iran-q1-2026-and-forecast>.
 33. Ibid.
 34. Ibidem.
 35. “Earth Orbit Passes 15,000 Active Satellites: Elon Musk’s Starlink Now Controls Two-Thirds of the World’s Active Satellite Fleet,” *LookUp*, June 2, 2026, <https://www.lookupspace.com/blog/earth-orbit-passes-15-000-active-satellites-elon-musks-starlink-now-controls-two-thirds-of-the-worlds-active-satellite-fleet>.
 36. Reha Kansara, “The Clandestine Network Smuggling Starlink Tech into Iran to Beat Internet Blackout,” *BBC*, May 2, 2026, <https://www.bbc.com/news/articles/cvgzk91leweo>.
 37. Alexander Ward and Robbie Gramer, “U.S. Smuggled Thousands of Starlink Terminals Into Iran After Protest Crackdown,” *Wall Street Journal*, February 12, 2026, <https://www.wsj.com/world/middle-east/u-s-smuggled-thousands-of-starlink-terminals-into-iran-after-protest-crackdown-69a8c74f>.
 38. Eva Dou and Faiz Siddiqui, “Iran Jams Starlink, Protesters’ Lifeline. Trump, Musk Say That Won’t Stand,” *Washington Post*, January 13, 2026, <https://www.washingtonpost.com/technology/2026/01/13/iran-starlink-protest-musk-trump/>.
 39. Chris Baraniuk, “GPS Jamming: The Invisible Battle in the Middle East,” *BBC*, March 9, 2026, <https://www.bbc.com/news/articles/c3ewwlx9e1xo>.
 40. Eva Dou and Faiz Siddiqui, “Iran Jams Starlink, Protesters’ Lifeline. Trump, Musk Say That Won’t Stand,” *Washington Post*, January 13, 2026, <https://www.washingtonpost.com/technology/2026/01/13/iran-starlink-protest-musk-trump/>.
 41. Supantha Mukherjee, Cassell Bryan-Low, and Parisa Hafezi, “Iranians Tap Musk’s Starlink to Skirt Internet Blackout, Sources Say,” *Reuters*, January 13, 2026, <https://www.reuters.com/business/media-telecom/iranians-tap-musks-starlink-skirt-internet-blackout-sources-say-2026-01-12/>.
 42. “Price of Musk’s Starlink Kits in Iran Soars as US Threatens War,” *Al Arabiya*, February 23, 2026, <https://english.alarabiya.net/News/middle-east/2026/02/23/price-of-musk-s-starlink-kits-in-iran-soars-as-us-threatens-war->.
 43. Samya Kullab, “Iranians Cross into Northern Iraq for Cheaper Food, Internet and Work after Border Reopens,” *Washington Times*, March 15, 2026, <https://www.washingtontimes.com/news/2026/mar/15/iranians-cross-northern-iraq-cheaper-food-internet-work-border/>; Feng, “Iranians Are Leaving the Country Just to Access the Internet.”
 44. Feng, “Iranians Are Leaving the Country Just to Access the Internet.”
 45. Samira Hosseini, “Exclusive: Iranians Risk Arrest at Iraq Border to Escape Tehran’s Total Internet Blackout,” *Euro News*, May 8, 2026, <https://www.euronews.com/2026/05/08/exclusive-iranians-risk-arrest-at-iraq-border-to-escape-tehrans-total-internet-blackout>.
 46. “Iran Restores Internet after 88-Day Blackout, Keeps Social Media Blocked,” *Iran International*, May 26, 2026, <https://www.iranintl.com/en/202605251140>.
 47. Motamedi, “Frustration Grows as Iran’s Wartime Internet Shutdown Breaks Grim Record.”
 48. Ibid.
 49. Chiara Castro, “Iran’s Internet Shutdown Proves We Need to Go beyond Starlink and VPNS — This Tech Could Be the Solution,” *TechRadar*, April 1, 2026, <https://www.techradar.com/vpn/vpn-privacy-security/irans-internet-shutdown-proves-we-need-to-go-beyond-starlink-and-vpns-this-could-this-be-the-solution>.
 50. Mahdi Saremifar and Ahmad Ahmadian, “Direct-to-Cell Offers Iranians Future Hope, Not a Fix Today,” *Iran International*, June 27, 2026, <https://www.iranintl.com/en/202606260731>.
 51. Alex Webb, “KDDI Becomes the First Operator to Launch Direct-to-Cell Data Services – But Is It Overhyped?” Juniper Research, September 2025, <https://www.juniperresearch.com/resources/blog/kddi-becomes-the-first-operator-to-launch-direct-to-cell-data-services-but-is-it-overhyped>.
 52. “Read the Full Text of Trump’s Preliminary U.S.-Iran Agreement to End the War,” *NPR*, June 18, 2026, <https://www.npr.org/2026/06/18/nx-s1-5863027/us-iran-trump-memorandum-of-understanding-full-text>.
 53. Peter Baker, “Trump Says Fighting with Iran Has Resumed as He Orders Blockade and Tolls,” *New York Times*, July 13, 2026, <https://www.nytimes.com/2026/07/13/us/politics/trump-iran-ceasefire.html>.
 54. *Iran Human Rights, Internet Freedom, and Accountability Act of 2026*, S. 3900, 119th Cong. (2026), <https://www.congress.gov/bill/119th-congress/senate-bill/3900>.

PUBLIC DIPLOMACY PAPER

ABOUT THE FUTURE OF PUBLIC DIPLOMACY PROJECT

Official outreach to foreign publics represents one of the most potent instruments of “soft power” available to the United States. Yet U.S. public diplomacy has eroded significantly since its heyday at the height of the Cold War, when American broadcasts and messaging engaged foreign publics behind the Iron Curtain and played an integral role in shaping the ideas that brought down the Soviet bloc. Through a combination of bureaucratic reshuffling and official neglect, the post-Cold War era has seen an erosion of the efficiency, strategic vision and impact of American strategic communications. Rebuilding the vibrancy, impact and persuasive potential of U.S. broadcasting is critical to ensuring the resonance of our ideas and values in today’s increasingly crowded, contested information space. The American Foreign Policy Council’s Future of Public Diplomacy Project is designed to elevate the profile of public diplomacy in the U.S. public policy debate, as well as to highlight to policymakers and the general public the various contemporary challenges now confronting American outreach.

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.

AFPC MISSION STATEMENT

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

1. Providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
2. Arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
3. Fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.



The American Foreign Policy Council

509 C Street NE
Washington, DC 20002
(202) 543-1006
Fax: (202) 543-1007
www.afpc.org

Mr. Herman Pirschner, Jr.
President

Mr. Ilan Berman
Senior Vice President

Mr. Richard M. Harrison
*Vice President of Operations and Director of
Defense Technology Programs*

Mrs. Annie Swingen
Vice President for External Relations

Dr. S. Frederick Starr
*Distinguished Fellow for Eurasia and Chairman
of the Central Asia-Caucasus Institute*

Dr. Svante E. Cornell
*Senior Fellow for Eurasia and Director of the
Central Asia-Caucasus Institute*

Ms. Laura Linderman
*Senior Fellow for Eurasia and Program Manager
of the Central Asia-Caucasus Institute*

Ms. Anna Harvey
Research Fellow and Program Officer

Ms. Calla O’Neil
Research Fellow and Program Officer

BOARD OF ADVISORS

Amb. Paula J. Dobriansky, PhD.
Hon. Christopher Ford, PhD.
Amb. James S. Gilmore, III
Hon. Newt Gingrich
Hon. Michelle S. Guida
Sen. Robert Kasten, Jr.
Amb. Richard McCormack
Gov. Thomas J. Ridge
Dr. William Schneider, Jr.
Hon. Manisha Singh
Hon. Dov Zakheim