Excerpt from InterAgency Journal 16-2
©2026 - Simons Center

Disclaimer: The articles published in the IAJ represent the opinions of the authors and do not reflect the official views of any United States government agency, the Department of War, the Department of the Army, the U.S. Army Command and General Staff College, the Command and General Staff College Foundation and Alumni Association, the Simons Center, or any other non-government, private, public or international organization.

The Threshold Problem:

Internet Freedom, Economic Pressure, and the *Missing Owner* in the 2026 Iran War

by Celia D. Hanley

When Iran cut its population off from the global internet in January 2026, and again for nearly three months after the U.S.-Israeli strikes of February 28, 2026, the United States (U.S.) had a statutory mandate, a network of grantees, a sanctions license written for communications tools, and money to help Iranians stay connected. It did not have an owner. This paper examines a single interagency seam in depth: The point where internet-freedom policy, run through the State Department and the U.S. Agency for Global Media, meets sanctions policy, run through the Treasury Department, while the Department of Defense shapes the same communications environment through military operations and counterintelligence risk falls between them all. Four decision points between January and September 2026 show the same pattern. Each department acted within its own authorities, no official was charged with weighing the tradeoffs across them, and the cost fell on Iranian civilians who had no voice in the decision. The paper proposes a named owner with three objective triggers and assesses how far pending legislation would go toward that fix.

Introduction

In mid-February 2026, with most of Iran's roughly ninety million people restricted to a heavily filtered network, the Open Technology Fund reported that demand in Iran for the U.S.-funded censorship-circumvention tools it supports had risen from seven-and-a-half million users to twenty-five million.[1] The fund needed about $10 million to keep up. Its board chair said the State Department had already found the money. The U.S. Agency for Global Media (USAGM), the agency through which the money had to pass, wrote that the usual funding route would take months and suggested the fund draw instead on its own annual appropriation. Two senators answered in writing

Celia D. Hanley is the founder and president of CatalinaIQ (Catalina Intelligent Solutions LLC), an intelligence-led risk management firm. Her 40-year career spans the CIA (Senior Operations Officer, 1985–1999), U.S. Army Counterintelligence (Special Agent, 2003–2005), the Defense Intelligence Agency (DIA Senior HUMINT Operations Officer and Program Manager, 2005–2021, including Chief of Staff, Defense Clandestine Service), and Raytheon (Associate Director, International Security, 2022–2025). She holds an master's in National Security Studies from American Military University, and her book, *Burned at First Light*, is forthcoming.

that advancing the fund's existing budget was not surge funding and would take support away from users in China, Cuba, and Russia.[2] Every party said it supported the goal. None had the authority to make the others move.

That episode is the argument of this article in miniature. The U.S. entered the 2026 Iran war with a law directing the Secretary of State to plan for an Iranian internet blackout, an established set of grantees, a Treasury license written to let communications tools reach Iranians, and bipartisan congressional support. What it lacked was a single official who owned the question of how hard Washington should work to keep Iranians connected and who could weigh that question against the government's other objectives in Iran. When the question arrived, each department answered the part in front of it. The parts did not add up.

In this context the word "threshold" is used for the point where one department's legitimate objective crosses into another's. Internet freedom and maximum economic pressure are both defensible policies. They are administered by different departments under different statutes, and in 2026 they collided at a point no one was assigned to manage. Absent an owner at that threshold, the decision is made by whichever department acts first, and the people who bear the cost are not in the room.

The analysis proceeds in four steps. It maps who held which authority before the crisis. It examines four decision points between January and September 2026, asking at each what happened, who should have decided, what an accountable owner would have done differently, and what leaders owed the people affected. It then assesses legislation pending in Congress that would partly close the gap. It closes with a proposal: A named owner, three objective triggers, and a counterintelligence review built into the process from the start.

The Authority Map Before the Crisis

Practitioners often observe that there is no interagency as such. There are departments and agencies, each with its own statutes, budgets, and habits, whose representatives meet as a body when a problem demands it. Each brings its own authorities to the table and leaves with them. The Iran connectivity problem fits that description closely. Before 2026, at least five sets of authorities touched it, and none was designed to override the others.

Practitioners often observe that there is no interagency as such.

The first sat with the State Department. In December 2024, Congress directed the Secretary of State to produce a strategy for internet freedom in Iran that would assess the Iranian government's ability to cut off all access to the internet and set out a strategy to circumvent blackouts for Iranian civil society. The same law authorized a grant program of $15 million a year for fiscal years 2025 and 2026.[3] State also funds circumvention through its Bureau of Democracy, Human Rights, and Labor and the Near East Regional Democracy program.[4]

The second sat with the USAGM and its grantee, the Open Technology Fund. Congress funds the fund through the USAGM, and since 2022 State has routed its own internet-freedom money to the fund through the same channel, a transfer the fund's president said normally takes one to two weeks.[5] That channel was already under strain. In March 2025, the USAGM terminated the fund's grant agreement; the fund sued, the termination was rescinded, and payments were again withheld until a federal court ordered them released.[6] In February 2026, The Guardian reported that the main granting office of the government's broader internet-freedom program had issued no new grants in 2025.[7]

The third sat with the Treasury Department. Iran is under comprehensive U.S. sanctions, so getting any technology to Iranians depends on a license. Since 2022, Treasury has authorized the export of certain services, software, and hardware incident to communications, first through Iran General License D-2, which it issued explicitly to support internet freedom after the Iranian government cut access during the protests of that year, and since May 2024 through a standing regulation, 31 C.F.R. § 560.540, which absorbed that license.[8] Anything beyond the terms of the license requires a specific license from the Office of Foreign Assets Control (OFAC).

On January 8, 2026, as nationwide protests intensified, the Iranian government imposed a near-total internet blackout that took down even much of its domestic network.

The fourth authority was diffuse. The counterintelligence risk created by sending tools into a country whose intelligence services actively hunt for them did not belong to any of the three. Iran's Ministry of Intelligence and Security had already shown how it would exploit demand for circumvention. A week after the June 2025 Israel-Iran war began, researchers at Lookout identified new samples of Android surveillanceware attributed to the ministry-linked group MuddyWater, disguised as VPN applications, one of them uploaded under a Starlink-themed file name that the researchers said may indicate Starlink lures.[9] The intelligence was public. The responsibility for acting on it, in the design of U.S. programs, was not assigned.

The fifth sat with the Department of Defense. Defense runs no internet-freedom program, but in wartime it is the department most able to change Iran's communications environment. Briefing reporters two days into Operation Epic Fury, the Chairman of the Joint Chiefs of Staff, General Dan Caine, said that "coordinated space and cyber operations effectively disrupted communications and sensor networks" across the theater, describing the aim in military terms as leaving Iran unable to see, coordinate, or respond.[10] Those operations served the strike campaign, and it was the Iranian government, not the U.S., that cut its own population off. But when one department degrades an adversary's networks while another works to keep that adversary's civilians online, both are operating at the same threshold. The public record shows no forum in which the two efforts were weighed together.

Decision Point One: The January Surge

On January 8, 2026, as nationwide protests intensified, the Iranian government imposed a near-total internet blackout that took down even much of its domestic network.[11] A phased restoration began on January 17, but it did not restore the internet Iranians had known. Monitoring by Filterwatch found that by late January the state had moved to a whitelisted model, blocking the global internet by default and admitting only approved services, with traffic at about a quarter of pre-shutdown levels.[12] Circumvention tools became the main route to the outside world, and demand for U.S.-funded tools more than tripled.

The response stalled for the reasons described above. On January 28, a bipartisan group of senators urged Secretary of State Marco Rubio to surge resources to internet-freedom programs for Iran.[13] State identified $10 million. The USAGM proposed an alternative the senators rejected. The fund warned that without the money it would have to cut off millions of users. Public reporting does not show when, or whether, the surge funds reached the fund.

Who should have decided? The statute gave

the Secretary of State the strategy, but the money had to pass through an agency whose leadership had tried a year earlier to terminate the fund's grant. Neither the Secretary nor the USAGM leadership could resolve the disagreement alone, and no one above them was charged with doing so on a timeline that matched the crisis. An accountable owner would have settled the surge mechanism in advance, before any blackout, so that the only decision required in January was whether conditions met a predefined trigger.

What leaders owed in this moment is not complicated. Millions of Iranians had already come to depend on these tools, and a sudden withdrawal would push them toward the informal market, where insecure VPNs are sold and the regime's surveillance can follow.[14] An unresolved funding dispute in Washington translated directly into exposure for people in Iran. Settling the mechanism before the crisis would not have required any official to take a new policy position. It would have required someone to own the plumbing.

Decision Point Two: The Starlink Substitution

While the funding dispute played out, the State Department made a different bet. According to U.S. officials who spoke to the *Wall Street Journal*, the department bought nearly 7,000 Starlink satellite terminals, most of them in January, and the U.S. smuggled roughly 6,000 into Iran after the crackdown, the first time Washington had directly sent Starlink equipment into the country. To pay for the terminals, the department redirected internet-freedom funds and allowed funding to lapse for two of the five VPN providers it supported for Iran.[15]

The logic of the bet is easy to see. During a full terrestrial shutdown, VPNs fail. Satellite terminals do not, at least until they are jammed or found. The costs are equally easy to see. A terminal is a physical object that must cross a border, be concealed, and be powered and pointed at the sky. Iranian police reported in August that they had seized 997 Starlink devices and detained 163 people in the preceding four months, with the equipment entering through border regions and southern maritime routes.[16] A VPN subscription paid from Washington reaches millions of users at little individual risk. A terminal reaches a household and places its owner in jeopardy.

Both instruments have a place. The interagency problem is that the choice between them was made inside one department, by redirecting money from one tool to another, without any visible process for weighing what was lost against what was gained. The tradeoff had at least three dimensions: coverage, since thousands of terminals cannot replace a VPN network serving millions; counterintelligence, since a smuggling chain is a supply chain the adversary will try to penetrate and the adversary appeared already to be using the Starlink name as bait; and the safety of recipients, who face arrest for possession. Public reporting does not indicate whether a counterintelligence assessment of the distribution chain preceded the shipments. The more important point is that no standing rule required one. As discussed in Section VII, pending Senate legislation would for the first time require that supported technologies be assessed for detectability, supply-chain risk, and the safety of users. That Congress saw a need to write this down suggests it was not routine practice.

...the U.S. smuggled roughly 6,000 [Starlink satellite terminals] into Iran after the crackdown, the first time Washington had directly sent Starlink equipment into the country.

A reader might object that "no visible

process" means only "no unclassified process." The *Journal* described the shipments as covert, and covert action carries its own approval machinery: A written presidential finding and notification of the congressional intelligence committees. The *Journal's* sources did not say whether the President or someone else approved the plan, and reported that senior appointees chose to divert the money from other internet-freedom programs.[17] Even if a finding existed, it would answer a different question. A finding authorizes an activity. It does not require anyone to weigh the coverage lost when two VPN providers went unfunded, to reconcile the shipments with Treasury's licensing posture, or to account for the exposure of the people receiving the terminals. A classified approval can settle who may act without settling who owns the tradeoff.

When U.S. and Israeli strikes opened Operation Epic Fury on February 28, the Iranian government imposed a complete blackout…

An owner would not necessarily have made a different choice. An owner would have made it with the coverage loss, the counterintelligence exposure, and the risk to recipients on the same page, and would have been accountable for the result. Leaders who choose to move risk from a program onto the people it is meant to help owe those people that accounting.

Decision Point Three: The Wartime Blackout

When U.S. and Israeli strikes opened Operation Epic Fury on February 28, the Iranian government imposed a complete blackout, just as the January restrictions had begun to ease.[18] It lasted eighty-eight days. Access began returning in the last week of May, but service was slow, popular platforms remained restricted, and senior officials had been issued SIM cards granting them access to the global internet that ordinary Iranians lacked.[19] The Armed Conflict Location and Event Data (ACLED) Project observed in early June that the VPNs many Iranians had relied on were no longer effective or affordable.[20]

This was the scenario the 2024 statute anticipated. It required an assessment of the Iranian government's ability to cut off all access and a strategy to circumvent blackouts. Whether that strategy was ever completed is not clear from the public record. What is clear is that when the blackout arrived, the tools available could not reach most of the population. Vice Admiral Jeff Trussler (ret.), a former Deputy Chief of Naval Operations for Information Warfare, and Sarah Havdala of the Jewish Institute for National Security of America concluded that the U.S. was unprepared to help Iranian civilians resist the shutdown, noting that VPNs cannot operate during a full terrestrial blackout and that Starlink terminals are difficult to smuggle and conceal.[21]

A strategy assigned by statute is not the same as an owner with resources and triggers. The statute told the Secretary what to plan for. It did not specify who would act when the plan was needed, what money would move automatically, or how the plan would account for the reconnection period, when a population returning from months of isolation is most exposed to manipulation. Trussler and Havdala reported that the regime has since offered a filtered, tiered service it calls "Internet Pro" to selected groups while retaining the ability to impose another nationwide blackout.[22] The government that controls who reconnects, and on what terms, also controls what they see first.

The ethical obligation here runs past the blackout itself. A government that spends years telling a population it stands with them, and funds their access to the outside world, takes on a duty to plan for the moment that access is cut. Meeting that duty requires a standing plan with

an owner, not a strategy document.

Decision Point Four: Economic Outcast Meets Internet Freedom

On August 24, 2026, the Treasury Department launched Operation Economic Outcast, which it describes as an unprecedented, whole-of-government economic campaign against Iran and its enablers, to continue until Iran ceases to pursue nuclear and conventional weapons capabilities and stops actively obstructing the Strait of Hormuz.[23] The same day, OFAC indefinitely suspended five general licenses, including those authorizing certain educational activities, noncommercial personal remittances, and academic exchanges.[24] On September 10, OFAC adopted a presumption of denial for Iran-related specific license requests. Licenses may now be issued only as required by law or in exceptional and urgent circumstances, such as risk to life, limb, or environmental safety, and OFAC reviews each application case by case in consultation with the State Department.[25] The campaign has continued through the autumn with further designations in October and November.[26]

The communications authorization in section 560.540 was not among the suspended authorizations, so the standard communications tools it covers remain authorized. Anything beyond its terms now meets a presumption of denial. That matters because the most promising responses to a full blackout fall outside routine exports. Trussler and Havdala recommend that OFAC quickly license distributors to move direct-to-cell-compatible phones and related products to civilians in restrictive countries.[27] Under the September policy, such a request would have to show exceptional and urgent circumstances to succeed.

Both policies are legitimate. Maximum economic pressure is an established instrument of coercion, and helping a population communicate with the outside world serves long-standing U.S. interests. The interagency failure is that no official owns the point where they meet. Treasury's licensing officers are not charged with weighing the consequences of a denial for Iran's information environment. The State Department is consulted on individual applications, but the text of the licensing policy contains no carve-out for communications and does not mention internet freedom. Applications are judged one at a time, after the policy is set, by officials whose mandate is pressure.

Maximum economic pressure is an established instrument of coercion, and helping a population communicate with the outside world serves long-standing U.S. interests. The interagency failure is that no official owns the point where they meet.

The cost of that arrangement falls on people who have no seat in any of the meetings where it is decided. A licensing policy is not the place to resolve a conflict between two national objectives, because the policy can only express one of them. The conflict has to be resolved above it, by someone with authority over both.

Congress Has Noticed, but the Seam Remains

Congress has seen at least part of the problem. The Iran Human Rights, Internet Freedom, and Accountability Act of 2026, introduced in February by Senator Dave McCormick and a bipartisan group of cosponsors, was ordered reported by the Senate Foreign Relations Committee on June 17, 2026 and formally reported in July.[28] The bill as introduced would have made the Secretary of State the federal official with primary responsibility for coordinating all federal efforts on digital freedom in Iran, and would have

directed the Secretary to work with Treasury and Commerce to ensure that sanctions enforcement does not impede companies providing Iranians the tools to reach the open internet.[29]

The committee's substitute moves in the right direction in one important respect and steps back in another. It adds a requirement that any technology supported under the bill be assessed for user safety, detectability by hostile governments, supply-chain risk, sanctions and export-control compliance, and risk of diversion to the Iranian government or the Islamic Revolutionary Guard Corps. That is the counterintelligence review missing from the Starlink decision. But the substitute also softens the ownership provision: the Secretary of State is now "authorized to be" the official with primary responsibility rather than designated as that official. It adds a savings clause providing that nothing in the bill authorizes any transaction prohibited by the Iranian sanction regulations except under a license.[30] The public record available at this writing shows no floor action in either chamber.

An official authorized to coordinate, but not required to, and with no mechanism to resolve a dispute with another department, is a coordinator in name.

Congress has also moved on the funding bottleneck behind the first decision point. On June 17, Senator Marsha Blackburn and a bipartisan group of six cosponsors filed the Open Technology Fund Reauthorization Act as an amendment to the Senate's FY2027 defense authorization bill. It would affirm the fund as an independent nonprofit corporation authorized to receive appropriations from Congress, strike the USAGM chief executive's role from the fund's governing statute, and repeal the fund's current section of the International Broadcasting Act.[31] Its fate depends on the defense bill. The House passed its version in July, but a motion to proceed to the Senate bill failed on July 14, and a final text is expected to be negotiated in the lame-duck session.[32] The most direct fix yet proposed for the January standoff is, for now, riding on the defense bill.

The savings clause in the Iran bill is sound law; Congress should not open a backdoor around sanctions in an internet-freedom bill. But it confirms that neither measure moves the threshold. Freeing the fund from the USAGM would shorten the funding chain without deciding when money should move. Under the Iran bill, the Secretary of State would coordinate internet-freedom efforts, Treasury would continue to set licensing policy, and a conflict between them would still have no designated forum or deadline. An official authorized to coordinate, but not required to, and with no mechanism to resolve a dispute with another department, is a coordinator in name. The bills improve the plan. They do not yet create the owner.

A Named Owner and Three Triggers

The fix proposed here builds on the pending bills rather than replacing them. Its purpose is to convert each of the ambiguities described above into a specific official's job, with an objective trigger and a documented decision.

The first element is a named owner. The Secretary of State should be required, not authorized, to designate a single senior official responsible for civilian connectivity in Iran, with a standing seat at the National Security Council deputies level for any Iran decision that affects it. When that official and Treasury disagree on a licensing question touching communications, the disagreement should go to the deputies within a fixed period, such as seventy-two hours, and the outcome should be recorded and reportable to the relevant committees. This does not take

licensing authority from Treasury. It ensures that when two national objectives collide, someone with authority over both decides, on a deadline, and on the record.

The second element is three triggers, each tied to an observable event rather than to a judgment made under pressure. The first trigger is a nationwide shutdown. When monitoring organizations document a nationwide or near-nationwide blackout in Iran, pre-appropriated surge funds for circumvention grantees should move through a funding channel agreed in advance, without a new interagency decision. This addresses the first and third decision points. In January 2026, it would have replaced weeks of correspondence with a transfer.

The second trigger is a new pressure campaign. Before any Iran sanctions action changes the licensing posture, Treasury and the designated owner should certify the scope of a communications carve-out and publish it with the action. This does not dilute economic pressure. It settles in advance which communications activity is protected, so that the boundary is drawn deliberately rather than discovered through denied applications. In August 2026, it would have produced a published statement on distributor licensing for satellite-capable devices, whichever way the decision went.

The third trigger is any U.S.-supported distribution of physical devices, or any shift of money from one class of circumvention tool to another. Either should require the assessment the Senate substitute describes, covering detectability, supply-chain risk, recipient safety, and diversion, together with an explicit statement of coverage lost and gained. The assessment should include the counterintelligence community from the start, since the adversary's interest in these supply chains is documented. In January 2026, it would have put the loss of two VPN providers and the exposure of terminal recipients in front of a decision-maker before the terminals were purchased.

The Department of Defense belongs in this process in three ways. First, the designated owner should see planned non-kinetic effects against Iranian communications infrastructure in time to register the connectivity objective at the deputy level, before execution where operational timelines permit. Second, the Joint Staff, U.S. Cyber Command, and U.S. Space Command should provide the owner with technical assessments of jamming, detection, and resilience for any circumvention technology the United States supports, the kind of analysis the Senate substitute already requests for direct-to-cell systems.[33] Third, Defense counterintelligence should join the review under the third trigger whenever a distribution chain crosses a combatant command's area of responsibility. None of this gives Defense a veto over internet-freedom programs or the owner a veto over military operations. It ensures that the department most able to change the communications environment is at the table when the threshold is crossed.

...when two national objectives collide, someone with authority over both decides, on a deadline, and on the record.

A reconnection plan should accompany all three triggers. The weeks after a blackout lifts are when a population is most exposed to manipulation and when the regime decides who gets access on what terms. The owner should be responsible for a plan that covers that period, including warnings about regime-controlled applications of the kind the Senate bill already contemplates.

None of this guarantees good outcomes. The tradeoffs between coverage and security, and between pressure and access, are real and will remain contested. What the framework changes is who makes them, when, and with

what accountability. Each decision point in 2026 was decided by default, by whichever office held the money or the license at the moment the question arrived. Under this framework, each would have been decided in advance by an identifiable official who answered for the result.

Conclusion: What Leaders Owed

As of early November 2026, the war is in its ninth month. A U.S. blockade of Iranian ports remains in place, indirect talks through Qatari mediators continue, and U.S. forces struck Iranian targets near the Strait of Hormuz on November 2, the eve of the midterm elections.[34] The next day, Iranian media reported internet outages in parts of Tehran and slowdowns elsewhere in the country.[35] Whether or not that episode grows, the regime has shown that it can and will cut access again. The question this paper has examined is not historical.

The ethical lesson of the Iran connectivity case is less about the quality of any single decision than about whether leaders treated a known ambiguity as unfinished business or as someone else's problem. Every department involved had a defensible position. Treasury was pursuing a policy of maximum pressure set at the highest levels. State was trying to reach Iranians with the tools and money it could find. The USAGM was operating under direction to shrink. Defense was fighting a war. Congress was writing letters and drafting bills. The failure was that no one was responsible for the whole, and the people who paid for that failure were Iranians who had trusted U.S. tools to keep them connected and, in some cases, accepted personal risk to use them.

The same pattern appears elsewhere in the war's record, in the dispute over the War Powers Resolution's clock, in allied basing and consultation, and in the government's response to cyber retaliation against U.S. companies. Each deserves its own study. The connectivity case is offered here as the clearest example because the remedy is within reach. The authorities exist. The grantees exist. A bill that would name an owner has already cleared committee, and a provision that would free the fund from the USAGM is pending on the defense bill. What remains is to make ownership mandatory, give the owner triggers that act before the next blackout, and require that the people who bear the risk of U.S. programs have their exposure weighed by someone accountable for it. The next threshold will arrive on its own schedule. The decision about who owns it can be made now.

Disclaimer: All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the U.S. Government. Nothing in the contents should be construed as asserting or implying U.S. Government authentication of information or endorsement of the author's views.

Notes

1 Magdalena Del Valle and Eric Martin, "Iran's Internet Goes Dark as US Agencies Spar on VPN Funding," *Bloomberg*, February 14, 2026, https://www.bloomberg.com/news/articles/2026-02-14/iranian-internet-goes-dark-as-us-agencies-clash-over-vpn-funding; Associated Press, "Iranians Are Back Online after a Monthslong Shutdown but Face Heavy Restrictions," *NPR*, May 28, 2026, https://www.npr.org/2026/05/28/g-s1-124610/iranians-back-online.

2 Del Valle and Martin, "Iran's Internet Goes Dark."

3 22 U.S.C. § 8754a (enacted as sec. 5124 of the *National Defense Authorization Act for Fiscal Year 2025*, Pub. L. 118-159), https://www.law.cornell.edu/uscode/text/22/8754a.

4 James Lankford et al. to Marco Rubio, January 28, 2026, https://www.lankford.senate.gov/wp-content/uploads/2026/01/2026.01.28_Internet_Freedom_in_Iran.pdf.

5 Del Valle and Martin, "Iran's Internet Goes Dark."

6 *Open Technology Fund v. Lake*, No. 1:25-cv-00840 (D.D.C. filed March 20, 2025); case summary, Civil Rights Litigation Clearinghouse, https://clearinghouse.net/case/46258/.

7 Aisha Down, "US Funding for Global Internet Freedom 'Effectively Gutted,'" *The Guardian*, February 19, 2026, https://www.theguardian.com/world/2026/feb/19/us-funding-for-global-internet-freedom-effectively-gutted.

8 U.S. Department of the Treasury, "U.S. Treasury Issues Iran General License D-2 to Increase Support for Internet Freedom," press release JY0974, September 23, 2022, https://fraser.stlouisfed.org/files/docs/publications/treaspr/2022/2022-09-23_jy0974.pdf; Office of Foreign Assets Control, "Iran-Related FAQs Updated May 16, 2024" (incorporating GL D-2 into 31 C.F.R. § 560.540), U.S. Department of the Treasury, https://ofac.treasury.gov/faqs/updated/2024-05-16.

9 Lookout Threat Intelligence, "Lookout Discovers Iranian APT MuddyWater Leveraging DCHSpy During Israel-Iran Conflict," July 21, 2025, https://security.lookout.com/threat-intelligence/article/lookout-discovers-iranian-dchsy-surveillanceware.

10 Brandon Vigliarolo, "Cyberwarriors Elevated to Big Leagues in US War with Iran," *The Register*, March 3, 2026, https://www.theregister.com/security/2026/03/03/top-general-spotlights-cyber-role-in-iran-conflict/4869319; David DiMolfetta, "Cyber, Space Commands Were among 'First Movers' in Strikes on Iran: Top General," *Defense One*, March 2, 2026, https://www.defenseone.com/threats/2026/03/cyber-space-commands-were-first-mover-strikes-iran-top-general/411819.

11 "Iran Experiencing Nationwide Internet Blackout, Monitor Says," *Al Jazeera*, January 8, 2026, https://www.aljazeera.com/news/2026/1/8/iran-experiencing-nationwide-internet-blackout-monitor-says; Narges Keshavarznia, "A Month of Iran's Internet: From Regional Disruptions and Blackouts to a New Whitelisted Reality," *Filterwatch*, January 28, 2026, https://filter.watch/english/2026/01/28/network-monitoring-january-2026-from-regional-disuptions-to-total-blackout-and-whitelisted-access/.

12 Keshavarznia, "A Month of Iran's Internet."

13 Lankford et al. to Rubio.

14 Jeff Trussler and Sarah Havdala, "The US Needs an Information-Warfare Strategy for Iran, and Beyond," *Breaking Defense*, September 21, 2026, https://breakingdefense.com/2026/09/the-us-needs-an-information-warfare-strategy-for-iran-and-beyond/.

15 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.

16 "Iran Seizes Nearly 1,000 Starlink Devices in 4 Months: Report," *Türkiye Today*, August 23, 2026, https://www.turkiyetoday.com/region/iran-seizes-nearly-1000-starlink-devices-in-4-months-report-3226667; Trussler and Havdala, "US Needs an Information-Warfare Strategy."

17 Ward and Gramer, "U.S. Smuggled Thousands of Starlink Terminals"; 50 U.S.C. § 3093(a), (c), https://www.law.cornell.edu/uscode/text/50/3093.

18 Associated Press, "Iranians Are Back Online."

19 Ibid.; Trussler and Havdala, "US Needs an Information-Warfare Strategy."

20 ACLED, "Has Iran Really Restored Internet Access?" Expert Comment, June 5, 2026, https://acleddata.com/expert-comment/has-iran-really-restored-internet-access.

21 Trussler and Havdala, "US Needs an Information-Warfare Strategy."

22 Ibid.

23 Office of Foreign Assets Control, "Statement of Licensing Policy on Iran-Related Requests," U.S. Department of the Treasury, September 10, 2026, https://ofac.treasury.gov/media/936916/download.

24 Office of Foreign Assets Control, "Suspension of Certain Iranian Transactions and Sanctions Regulations General Licenses," *Federal Register* 91, no. 164 (August 26, 2026), https://www.govinfo.gov/content/pkg/FR-2026-08-26/pdf/2026-17426.pdf.

25 Office of Foreign Assets Control, "Statement of Licensing Policy."

26 U.S. Department of State, "Iran Sanctions," accessed November 6, 2026, https://www.state.gov/iran-sanctions.

27 Trussler and Havdala, "US Needs an Information-Warfare Strategy."

28 Congress.gov, "S.3900, Iran Human Rights, Internet Freedom, and Accountability Act of 2026: All Actions," accessed November 6, 2026, https://www.congress.gov/bill/119th-congress/senate-bill/3900/all-info; U.S. Senate, *Iran Human Rights, Internet Freedom, and Accountability Act of 2026*, S. 3900, 119th Cong., 2d sess., reported July 27, 2026, https://www.congress.gov/119/bills/s3900/BILLS-119s3900rs.pdf.

29 U.S. Senate, *Iran Human Rights, Internet Freedom, and Accountability Act of 2026*, S. 3900, 119th Cong., 2d sess., introduced February 24, 2026, secs. 3(a)–(b), https://www.congress.gov/119/bills/s3900/BILLS-119s3900is.pdf.

30 U.S. Senate, *Iran Human Rights, Internet Freedom, and Accountability Act of 2026*, S. 3900, reported July 27, 2026, secs. 3(a), 4(c)(2)(D), 8; Senate Foreign Relations Committee, "S. 3900 (Reported Out)," https://www.foreign.senate.gov/download/s-3900-reported-outpdf.

31 S. Amdt. 5841 to S. 4784, *Open Technology Fund Reauthorization Act*, 119th Cong., 2d sess., *Congressional Record* 172 (June 17, 2026): S2904–S2905, https://www.congress.gov/amendment/119th-congress/senate-amendment/5841/text.

32 Congressional Research Service, *FY2027 NDAA: Status of Legislative Activity*, IN12704 (Washington, DC: Congressional Research Service, updated September 1, 2026), https://www.congress.gov/crs-product/IN12704; Michael Lowell et al., "Congress Returns: National Security and Trade Provisions to Watch in the FY2027 NDAA," *Reed Smith Trade Compliance Resource Hub,* November 2, 2026, https://www.tradecomplianceresourcehub.com/2026/11/02/congress-returns-national-security-and-trade-provisions-to-watch-in-the-fy2027-ndaa/.

33 U.S. Senate, *Iran Human Rights, Internet Freedom, and Accountability Act of 2026*, S. 3900, reported July 27, 2026.

34 Vaughn Cockayne, "U.S.-Iran Talks on Last-Minute Peace Plan Continue as Fears of Escalation Simmer," *Washington Times*, November 1, 2026, https://www.washingtontimes.com/news/2026/nov/1/us-iran-talks-last-minute-peace-plan-continue-fears-escalation-simmer/; "Iran Plays Down Hope for Deal to End War after New U.S. Strikes on Eve of Midterm Elections," *CBS News*, November 3, 2026, https://www.cbsnews.com/live-updates/iran-war-us-trump-negotiations-midterms/; Associated Press, "US Has Conducted Defensive Strikes on Iranian Targets in the Strait of Hormuz, US Official Says," November 2, 2026, https://apnews.com/article/iran-us-trump-netanyahu-israel-war-b4519ef86bafe2672e0855d7a48ce309.

35 "Internet Disruptions Reported in Tehran: Iranian Media," *APA*, November 4, 2026, https://en.apa.az/asia/internet-disruptions-reported-in-tehran-iranian-media-533832.