TAL SHIAR DEFENSE INTELLIGENCE REPORT

UNCLASSIFIED//AOR CENTCOM, IRAN

Starlink Proves Vital for Protestors Bypassing Iran's Internet Blackout

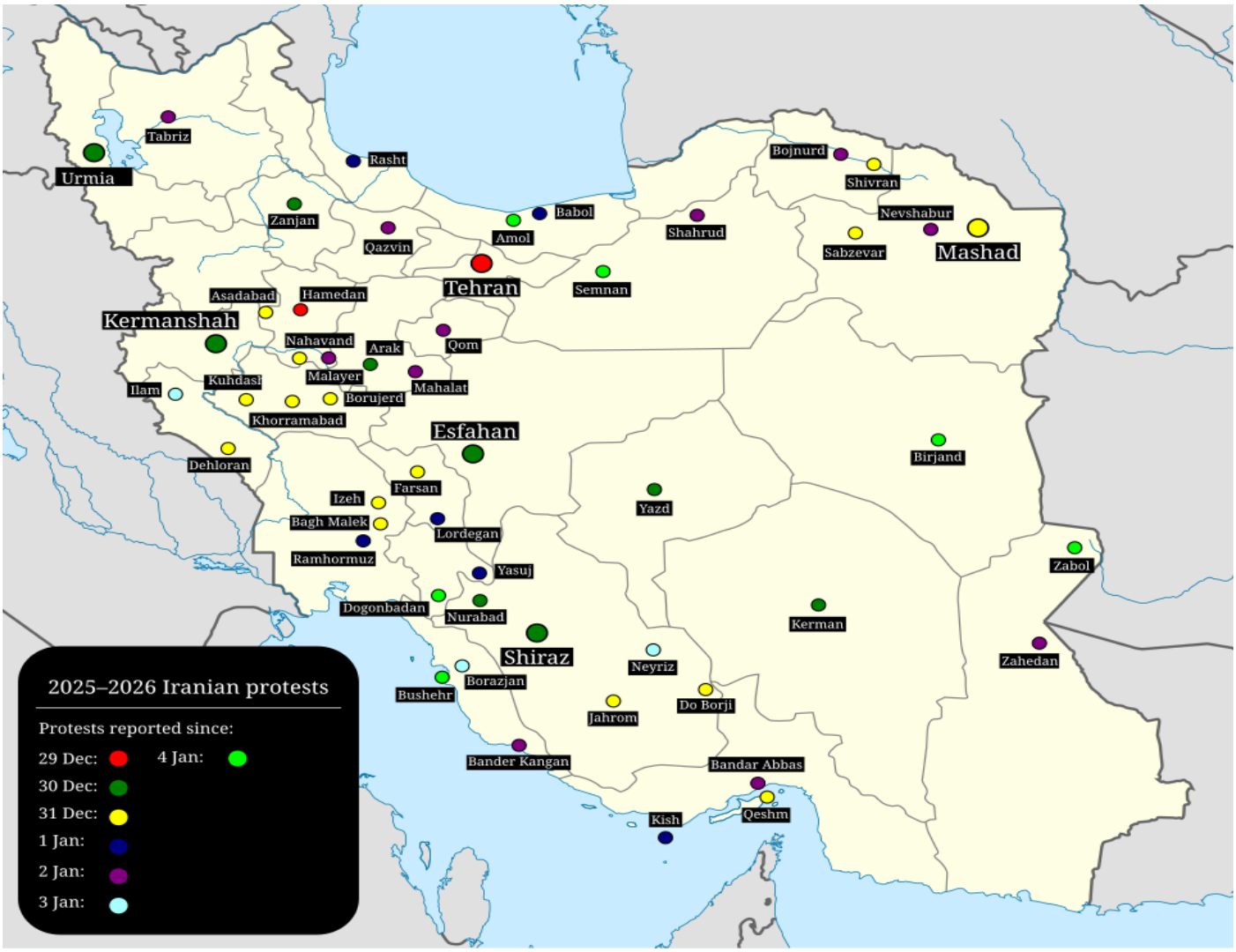
Prepared by Tal Shiar Directorate of Intelligence, 3 February 2026

Starlink satellite internet has served as a limited but strategically vital bypass to Iran's unprecedented nationwide internet and telecommunications blackout imposed on 8 January 2026. These systems enabled select activists, protesters, and journalists to document and transmit evidence of deadly security force crackdowns on widespread anti-regime demonstrations in late 2025. This has sustained some international visibility and scrutiny of reported human rights violations despite regime efforts to isolate the population of ~92 million, potentially amplifying pressure on Iranian authorities while exposing the growing disruptive power of commercial satellite constellations against state digital controls—though Iranian jamming and enforcement constrain its reach.

- Protests erupted 28 December 2025 in Tehran over economic crisis (currency collapse and inflation) and rapidly spread to dozens of cities and provinces with diverse participants chanting against the regime. Authorities imposed a near-total blackout on 8 January 2026 (dropping connectivity ~97%) to conceal lethal responses involving firearms, mass arrests and killings.

- Thousands of Starlink terminals (estimates ~50,000) have been active; SpaceX waived subscription fees for Iranian users around mid-January, allowing uploads of protest videos, casualty images, and coordination that became a primary information lifeline despite risks.

- Iranian authorities banned Starlink, threaten users with prison (up to 10 years), deploy military-grade jammers/GPS spoofing to degrade signals, and raid rooftops; only a small fraction of the population accesses it, but it proved crucial for activists amid the blackout lasting weeks (with partial, censored domestic access returning unevenly).



Countermeasures: Practical Ways Protesters Can Mitigate Iranian Regime Jamming of Starlink

Iranian forces have deployed military-grade GPS spoofing/denial (flooding L1 band) and direct RF jamming (targeting Ku/Ka-band signals with mobile units, including Russian-sourced systems like Krasukha-4 equivalents) to degrade Starlink connectivity, often reducing performance by 30-80% in targeted urban/protest zones and creating localized blackouts. While SpaceX implements software/firmware updates for adaptive defenses (e.g., GPS-independent satellite triangulation, frequency hopping, beam null-steering), protesters on the ground can apply practical, low-tech/user-level mitigations to improve reliability, minimize detection, and sustain brief connectivity windows for uploading evidence or coordination—though no method fully defeats high-power jamming or physical raids, and use remains high-risk (up to 10-year prison sentences, drone surveillance, rooftop searches).

- **Leverage automatic firmware updates and brief activation windows**: Keep the Starlink app/device powered and connected during short, unpredictable periods of lower jamming (often at night or in less-targeted neighborhoods); terminals auto-download SpaceX patches that enable GPS bypass via constellation-based positioning (triangulation from Starlink satellites themselves) and counter jamming in real-time—users in affected areas report improved packet loss from ~35% to lower levels post-update.

Activate only for essential uploads (e.g., video evidence) to reduce on-air time and detection risk from RF scanners/drones.

- **Discreet terminal placement and physical shielding**: Mount dishes on rooftops or hidden elevated spots with clear sky view but camouflage (e.g., under tarps, in planters, or behind low walls) to evade visual drone/rooftop patrols; create partial Faraday-like shielding using metal mesh/open-top enclosures or sandbags around the dish to attenuate side-lobe jamming while preserving upward satellite links—some users report this reduces effective jammer impact in directional setups. Operate from dispersed, non-obvious locations (e.g., shared community terminals rotated among users) to avoid concentrated raids in high-footage areas.

- **Minimize exposure and combine with low-bandwidth/offline tactics**: Use Starlink sparingly for high-priority outbound traffic (compress videos, batch uploads); pair with mesh/Bluetooth offline tools (e.g., apps like Briar or Bridgefy for local coordination) or one-way satellite receivers (e.g., Toosheh for inbound news) to reduce reliance on two-way links vulnerable to jamming. Relocate terminals frequently if jamming intensifies or raids occur nearby, and avoid fixed patterns that security forces exploit via signal triangulation or protest-area targeting.

Conclusion

Protesters can partially counter regime jamming through disciplined operational security (brief activations, updates, shielding, relocation) and SpaceX's rapid software countermeasures, sustaining enough intermittent connectivity to document abuses and maintain information outflow amid the 2026 blackout. These tactics highlight Starlink's resilience as a decentralized tool against digital repression but underscore persistent vulnerabilities to localized electronic warfare and physical enforcement—success depends on user caution, terminal dispersion (~50,000 estimated units), and ongoing SpaceX adaptations, though regime escalation risks escalation of user endangerment and detection.

Tal Shiar was founded by Nadeem Iqbal, a national security expert who served over 16 years as an intelligence officer for the Department of Defense from 2006-2022. His career began as a counter-insurgency analyst on the Afghanistan-Pakistan Task Force (2006–2013), followed by 9 years as a military analyst in the Syria Branch (2013–2022). He deployed five times in support of combat operations (3× Afghanistan, 2× Iraq), including two rotations with Special Operations Forces focused on counter-terrorism missions in the CENTCOM theater. Additional roles included rotations to CIA Headquarters as the military analyst for the DNI Middle East Task Force and served as the Syria Country Director for Office of Secretary of Defense Policy (OSDP). He was recognized with Joint Civilian Commendation/Achievement Medals, the NATO Medal(x3), the Secretary of Defense GWOT Medal, DoD Expeditionary Award and the OSD Excellence Award.