INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-05 13:26 UTC

Iran Internet Shutdowns and Information Controls Amid Military Conflict (April 2026)

GOVERNANCE | HIGH

SCC Item ID	SCC-GOV-2026-0010
Type	Governance
Severity	HIGH
Affected Products	Iran national digital infrastructure, civilian communication services
Published	2026-04-04
Discovery Source	Gemini

Executive Summary

Iranian authorities have implemented broad internet shutdowns and tightened information controls amid active military conflict, cutting civilian communications infrastructure as a deliberate state-level tactic. Concurrently, CISA and the Canadian Centre for Cyber Security documented Iran-nexus offensive cyber operations targeting U.S. and allied infrastructure in February 2026, combining internal suppression with external cyber aggression. Organizations with operations in the region, exposure to Iranian-linked threat actors, or presence in targeted sectors such as energy and critical infrastructure should treat this as an active threat context requiring heightened monitoring. Confidence on the specific April 2026 shutdown event is medium; the broader Iranian cyber threat posture is corroborated by CISA primary sources.

Technical Analysis

No CVE or CVSS scoring applies to this item; it represents a geopolitical threat context rather than a discrete software vulnerability. The observed tactics map to three MITRE ATT&CK techniques: T1583 (Acquire Infrastructure), T1498 (Network Denial of Service), and T1562.001 (Impair Defenses: Disable or Modify Tools). Iranian state actors and IRGC-affiliated groups have historically combined infrastructure acquisition with disruptive network operations and defensive impairment against targets in the energy, government, and telecommunications sectors. The CCCS Cyber Threat Bulletin (February 2026) and CISA Iran Threat Overview identify Iran-nexus APT groups conducting espionage and disruptive operations against U.S. and allied infrastructure in direct response to U.S./Israel military action. Internet shutdown mechanics consistent with BGP route withdrawal and deep packet inspection-based throttling align with Iran's historical patterns during prior conflict periods (2019, 2022). No specific IOCs tied to the April 4 shutdown event are available from verified primary sources at time of writing.

Action Checklist

1. Step 1: Situational Awareness, Review CISA Iran Threat Overview (https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran) and the CCCS February 2026 bulletin for current Iranian TTPs. Brief your SOC on the elevated threat posture for critical infrastructure sectors, particularly energy.
2. Step 2: Detection, Activate or verify coverage for Iran-nexus TTPs: monitor for anomalous BGP route changes if you peer with regional providers, review firewall and proxy logs for traffic to/from Iranian IP space, and check for indicators of defensive impairment (T1562.001) such as unexpected agent or logging service terminations.
3. Step 3: Exposure Reduction, Audit external-facing assets for known Iranian threat actor targeting patterns documented in CISA advisories. Confirm multi-factor authentication is enforced on remote access and VPN infrastructure. Restrict or monitor access from geographic regions flagged in current advisories.
4. Step 4: Monitoring Posture, Increase log retention and alert sensitivity on OT/ICS environments and energy sector assets for the duration of the conflict period. Validate SIEM rules covering T1498 (volumetric anomalies) and T1583 (unusual infrastructure registration or C2 beaconing patterns).
5. Step 5: Post-Review, Evaluate whether your threat intelligence feeds include Iranian APT IOC sources (e.g., CISA advisories, CCCS bulletins). Identify control gaps in geopolitical threat monitoring and consider adding a standing Iran threat brief to your recurring threat intelligence cycle.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISA (1-888-282-0870) and senior leadership if: confirmed Iranian IP space connections to OT/ICS or energy sector assets are detected, logging or security agent terminations (T1562.001) are observed on critical infrastructure hosts, BGP route anomalies affecting your ASN or upstream providers are identified, or any VPN/remote access authentication is traced to Iranian IP ranges — all of which constitute potential precursor activity to the destructive ICS-targeting campaigns documented in the CCCS February 2026 bulletin.
Recovery Notes	Recovery monitoring for this threat must persist beyond the immediate conflict period, as Iranian APT groups (notably Tortoiseshell, APT33/Refined Kitten, and MuddyWater) have demonstrated pre-positioned access that activates weeks or months after initial intrusion. After implementing containment controls, verify OT/ICS historian and HMI integrity via file hash baselines compared against known-good states, and confirm no unauthorized scheduled tasks or persistence mechanisms (T1053, T1543) were installed on energy sector assets during the exposure window. Maintain elevated monitoring posture and extended log retention for a minimum of 90 days post-conflict-period, reviewing CISA and CCCS advisories weekly for new Iranian APT IOCs that may match artifacts already present in your retained logs.

Forensic Artifacts	Firewall and proxy connection logs filtered against Iranian-registered IP ranges (RIPE ASNs including AS44244 IRCell, AS56402 Fanava, AS60280 Shatel) for the 30-day window preceding detection activation — Iranian APT pre-positioning typically precedes overt action and will appear as low-and-slow reconnaissance in these logs | Windows System Event Log entries for Event IDs 7036 and 7040 on all hosts running security or logging agents, specifically capturing unexpected state changes to Sysmon, EDR, or SIEM forwarder services consistent with T1562.001 (Impair Defenses: Disable or Modify Tools) as documented in CISA Iran APT advisories | OT/ICS network DNS query logs from boundary resolvers and historians for the conflict monitoring period, focusing on low-TTL external domains, DGA-pattern hostnames, and DNS-over-HTTPS usage inconsistent with operational baselines — Iranian implant families documented by CISA use DNS for C2 beaconing | VPN and remote access authentication logs from the prior 30 days exported from the VPN concentrator (Cisco ASA show vpn-sessiondb, Fortinet FortiGate auth event logs, Pulse Secure admin logs) identifying any source IPs geolocating to Iran or authentication anomalies occurring outside business hours consistent with Iranian APT operational timing (UTC+3:30) | BGP route change records from your upstream provider or RIPE NCC RIS Live for your ASN covering the conflict period — Iranian state actors have historically used BGP hijacking for traffic interception against targeted organizations, and anomalous route advertisements involving your prefixes are direct forensic evidence of this technique

Per-Action IR Details

Step 1: Situational Awareness — Review CISA Iran Threat Overview (https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran) and the CCCS February 2026 bulletin for current Iranian TTPs. Brief your SOC on the elevated threat posture for critical infrastructure sectors, particularly energy.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability, maintaining threat awareness, and briefing response teams on current threat actor TTPs prior to an incident

Controls: NIST IR-4 (Incident Handling) — maintain an active incident handling capability aligned to current threat posture, NIST SI-5 (Security Alerts, Advisories, and Directives) — receive and act on CISA and CCCS advisories for Iran-nexus threats, NIST IR-2 (Incident Response Training) — brief SOC analysts on Iranian APT TTPs specific to energy and critical infrastructure targeting, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate geopolitical threat intelligence into vulnerability prioritization for energy sector assets

Compensating: For teams without a threat intelligence platform: download the CISA Iran APT advisory PDFs directly and extract IOC tables manually. Use a shared markdown or wiki page as a 'live TTP brief' that both analysts update daily during the conflict period. Pin CISA's Iran topic RSS feed (https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran) in your browser and set a calendar reminder for daily review. Distribute the TTP summary via email or Slack to on-call staff with a read-receipt or acknowledgment reply requirement.

Evidence: Before acting, document your current threat intelligence baseline: screenshot or export the current CISA Iran advisory page with timestamp, record the date of last CCCS bulletin review in your incident log, and note which SOC analysts were briefed and when. This establishes a preparedness timestamp if regulators or auditors later ask when your organization became aware of the elevated Iran threat posture. Retain the CCCS February 2026 bulletin PDF with file hash for evidentiary integrity.

Step 2: Detection — Activate or verify coverage for Iran-nexus TTPs: monitor for anomalous BGP route changes if you peer with regional providers, review firewall and proxy logs for traffic to/from Iranian IP space, and check for indicators of defensive impairment (T1562.001) such as unexpected agent or logging service terminations.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring for indicators of compromise, correlating network and host telemetry, and analyzing anomalous behavior consistent with known Iranian APT TTPs

Controls: NIST SI-4 (System Monitoring) — monitor for T1562.001 (Impair Defenses: Disable or Modify Tools) via unexpected termination of logging agents or EDR services, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review firewall and proxy logs for Iranian IP space traffic on a defined frequency elevated to continuous during conflict period, NIST AU-12 (Audit Record Generation) — ensure logging is active on all systems that could generate Iran-nexus indicators before detection begins, CIS 8.2 (Collect Audit Logs) — validate audit log collection is enabled across perimeter firewalls, proxies, and OT network boundaries before beginning log review

Compensating: BGP monitoring without enterprise tooling: subscribe to free BGPmon alerts (bgpmon.net) or use RIPE NCC's RIS Live BGP stream to watch for route hijacks involving your ASN or upstream providers. For Iranian IP space traffic: pull firewall deny/allow logs and run a one-liner against published Iranian IP ranges from RIPE (ASNs: AS44244, AS56402, AS60280 among others) — example bash: `grep -Ff iranian_asn_prefixes.txt firewall_export.csv | awk '{print $1, $5, $7}' > iran_hits.txt`. For T1562.001 detection without EDR: on Windows, query the System Event Log for Event ID 7036 (Service Control Manager — service state change) and Event ID 7040 filtering on your AV, Sysmon, or logging agent service names: `Get-WinEvent -LogName System | Where-Object {$_.Id -in @(7036,7040) -and $_.Message -match 'Sysmon|CrowdStrike|Splunk|WinCollect'}`

Evidence: Capture before and retain: firewall connection logs filtered for Iranian IP ranges (RIPE-registered Iranian ASN prefixes) covering the 72 hours prior to detection activation — Iranian APT pre-positioning activity often precedes overt action. Export proxy logs for the same window filtering on suspicious User-Agent strings associated with Iranian tooling (e.g., custom implants documented in CISA advisories). For T1562.001: pull Windows System Event Log entries for Event IDs 7036 and 7040 on all servers running logging or security agents, and capture a point-in-time snapshot of running services via `Get-Service | Where-Object {$_.Status -eq 'Stopped'}` on each endpoint, timestamped. On Linux hosts: `systemctl list-units --state=failed > failed_services_$(date +%Y%m%d_%H%M%S).txt`. Preserve these in write-once storage immediately.

Step 3: Exposure Reduction — Audit external-facing assets for known Iranian threat actor targeting patterns documented in CISA advisories. Confirm multi-factor authentication is enforced on remote access and VPN infrastructure. Restrict or monitor access from geographic regions flagged in current advisories.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Restricting attacker access, hardening exposed attack surfaces, and implementing network-level controls to limit blast radius during an elevated threat period

Controls: NIST IR-4 (Incident Handling) — execute containment actions consistent with the IR plan in response to confirmed elevated Iranian APT threat posture, NIST AC-17 (Remote Access) — enforce MFA on all VPN and remote access infrastructure targeted by Iranian credential-stuffing and spearphishing campaigns, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA on all externally-exposed enterprise applications given documented Iranian APT targeting of remote access infrastructure, CIS 6.4 (Require MFA for Remote Network Access) — require MFA for all remote network access, specifically VPN endpoints documented as Iranian APT initial access vectors, CIS 4.4 (Implement and Manage a Firewall on Servers) — implement firewall rules restricting inbound access from Iranian IP ranges on all external-facing servers

Compensating: MFA enforcement audit without IAM tooling: run `net user /domain` or query your VPN's authentication logs to identify accounts that authenticated via password-only in the last 30 days — flag these for immediate MFA enrollment. For geographic restriction without a commercial geo-IP firewall: use MaxMind's free GeoLite2 database with iptables or Windows Firewall rules. Example iptables block for Iranian IP blocks: `iptables -A INPUT -m geoip --src-cc IR -j DROP` (requires xtables-addons with GeoLite2). For external asset audit: run `nmap -sV --script=banner [your_external_ip_range]` to enumerate exposed services and cross-reference against CISA advisory-documented Iranian targeting vectors (RDP, VPN appliances, Exchange OWA, Fortinet SSL-VPN).

Evidence: Before implementing geo-restrictions or MFA changes: export a full list of successful VPN and remote access authentications from the prior 14 days, noting any authentications from Iranian IP ranges or unusual off-hours patterns. Pull authentication logs from your VPN concentrator (e.g., Cisco ASA: `show vpn-sessiondb` or Fortinet FortiGate authentication event logs filtered on source country IR). Capture a snapshot of your current firewall ruleset (`iptables -L -n -v > fw_rules_prechange_$(date +%Y%m%d).txt` or equivalent) before modification — this is your rollback baseline and evidence of pre-containment state. Document all accounts lacking MFA with a timestamped

export.

Step 4: Monitoring Posture — Increase log retention and alert sensitivity on OT/ICS environments and energy sector assets for the duration of the conflict period. Validate SIEM rules covering T1498 (volumetric anomalies) and T1583 (unusual infrastructure registration or C2 beaconing patterns).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Increasing monitoring fidelity, extending retention for forensic capability, and validating detection coverage against specific Iranian APT techniques targeting critical infrastructure

Controls: NIST AU-4 (Audit Storage Capacity) — increase audit log storage allocation to accommodate extended retention during elevated conflict-period threat posture, NIST AU-11 (Audit Record Retention) — extend log retention beyond standard policy for OT/ICS and energy sector assets for the duration of the active conflict period, NIST SI-4 (System Monitoring) — validate detection rules for T1498 (Network Denial of Service) and T1583 (Acquire Infrastructure) against known Iranian APT C2 and DDoS techniques, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — increase review frequency on OT/ICS network logs to continuous or near-real-time during elevated threat period, CIS 8.2 (Collect Audit Logs) — ensure audit log collection is validated and active on OT/ICS boundary devices, historians, and HMIs before increasing retention

Compensating: Without a commercial SIEM: deploy Sigma rules for T1498 and T1583 converted to native query syntax for your log platform. For T1498 volumetric detection with Wireshark or ntopng: set threshold alerts on interface packet-per-second rates exceeding 3x baseline on OT network segments. For T1583 C2 beaconing detection without EDR: use Zeek (free) on a network tap to generate conn.log and dns.log, then run a beacon analysis script — `zeek-cut id.orig_h id.resp_h duration` piped through a frequency analysis to flag hosts with regular outbound connection intervals (beaconing). For log retention on a budget: configure syslog forwarding from OT boundary devices to a local Linux host running rsyslog with a 90-day rotate policy: `$FileCreateMode 0640 / $DirCreateMode 0750` with daily rotation and gzip compression.

Evidence: Before increasing alert sensitivity: baseline your current false positive rate per rule to avoid alert fatigue masking real Iranian APT activity — export a 7-day alert count by rule from your current platform. For T1498 (volumetric anomalies): capture current network flow baselines from your OT/ICS network using NetFlow or sFlow exports — these are your comparison baseline if a DDoS or wiper-preceding traffic spike occurs. For T1583 (C2 infrastructure): pull current DNS query logs from your OT network's DNS resolvers for the prior 30 days, focusing on low-TTL domains and DGA-pattern hostnames consistent with Iranian APT implant families documented in CISA advisories (e.g., MURKYTOP, TURNEDUP). Store these baseline captures in write-once storage with SHA-256 hashes.

Step 5: Post-Review — Evaluate whether your threat intelligence feeds include Iranian APT IOC sources (e.g., CISA advisories, CCCS bulletins). Identify control gaps in geopolitical threat monitoring and consider adding a standing Iran threat brief to your recurring threat intelligence cycle.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Conducting lessons learned, identifying control and intelligence gaps, and improving the detection and intelligence cycle to address geopolitical threat actor coverage

Controls: NIST IR-8 (Incident Response Plan) — update the IR plan to incorporate geopolitical threat scenarios and standing intelligence requirements for Iranian APT activity, NIST IR-5 (Incident Monitoring) — document the gap in Iranian APT IOC coverage as a tracked finding with remediation timeline, NIST SI-5 (Security Alerts, Advisories, and Directives) — formalize intake of CISA and CCCS Iran-nexus advisories into the recurring threat intelligence cycle as standing requirements, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — update the vulnerability management process to include geopolitical threat actor targeting patterns as a prioritization input, CIS 7.2 (Establish and Maintain a Remediation Process) — document identified control gaps with risk-based remediation timelines in the formal remediation process

Compensating: For teams without a commercial TI platform: create a free MISP instance (misp-project.org) and subscribe to the CIRCL OSINT feed plus CISA's AIS (Automated Indicator Sharing) feed — both are free and include Iranian APT IOCs. Alternatively, use a structured markdown threat register updated weekly: columns for TTP (ATT&CK

ID), last observed date, IOC type, source advisory, and detection coverage status. Schedule a recurring 30-minute weekly calendar block titled 'Iran Threat Brief' for both analysts to review new CISA/CCCS publications and update the register. Use OpenCTI (free, open-source) as a lightweight alternative to commercial TI platforms for structured Iranian APT profile tracking.

Evidence: For the post-review, document as evidence: a gap analysis comparing your current TI feed IOC sources against the CISA Iran APT advisory IOC list — record which IOCs were in your feeds and which were missing. Export your SIEM or detection platform's rule coverage map against the MITRE ATT&CK techniques listed in the CISA Iran advisory (T1562.001, T1498, T1583) and document coverage gaps with timestamps. Retain all logs, alerts, and detection outputs from the conflict monitoring period for a minimum of 12 months per NIST AU-11 (Audit Record Retention) guidance, as Iranian APT campaigns have demonstrated long dwell times with delayed secondary actions.

Detection Guidance

No confirmed IOCs specific to the April 2026 shutdown event are available from primary sources. For the broader Iranian cyber threat context, detection should focus on: (1) T1498, monitor NetFlow and perimeter logs for volumetric anomalies consistent with denial-of-service activity; establish baselines now for comparison; (2) T1562.001, alert on endpoint security agent stops, Windows Event ID 7036 (service state change) for security tools, and auditd logs showing security daemon terminations on Linux hosts; (3) T1583, hunt for new or recently registered domains with Iranian-linked registration patterns in DNS query logs, cross-referenced against CISA-published Iran APT infrastructure indicators. Review CISA Iran Threat Overview for the most current IOC sets. Flag this item as monitor status; escalate to high if CISA or CCCS publish a specific advisory tied to April 2026 activity.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran`	CISA Iran Threat Overview — authoritative source for current Iranian APT IOCs and advisories; check for updates tied to April 2026 activity	HIGH
URL	`https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-response-usisrael-strikes-february-2026`	CCCS February 2026 bulletin on Iranian cyber threat response to U.S./Israel strikes — secondary source, T3 tier, human validation recommended	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1583** — Acquire Infrastructure
- **T1498** — Network Denial of Service
- **T1562.001** — Disable or Modify Tools

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1583	Acquire Infrastructure	Resource-Development
T1498	Network Denial of Service	Impact
T1562.001	Disable or Modify Tools	Defense-Evasion

Sources

Source	URL	Tier
Iranian Cyber Threat Response to US/Israel strikes, February 2026	https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-c...	T3
Iran Conflict Heightens Cyber Threats to U.S. Energy Infrastructure	https://www.csis.org/analysis/iran-conflict-heightens-cyber-threats...	T3
Iran-linked hackers raise threat level against US, allies	https://www.cybersecuritydive.com/news/iran-hackers-threat-level-us...	T3
Iran-linked cyber espionage surges across Middle East as conflict ...	https://industrialcyber.co/critical-infrastructure/iran-linked-cybe...	T3
Iran Threat Overview and Advisories - CISA	https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-p...	T1

Generated 2026-04-05 13:26 UTC by TJS Security Command Center